Forma B.V.
Argonstraat 5, 7463 PD Rijssen
KvK 42200208 · forma.nl

Verwerkersovereenkomst Forma B.V.

Versie 1.0, november 2026

Deze verwerkersovereenkomst hoort bij de overeenkomst tussen Forma B.V., Argonstraat 5, 7463 PD Rijssen, KvK 42200208 (“wij”) en de organisatie die onze offerte accepteert (“u”). Hij geldt vanaf het moment dat u de offerte accepteert. Begrippen als persoonsgegevens, verwerking en datalek hebben de betekenis uit de AVG.

1 Onderwerp en rollen

1.1 Wij bouwen, hosten en onderhouden apps voor u. Daarbij verwerken wij persoonsgegevens in uw opdracht. U bent verwerkingsverantwoordelijke, wij zijn verwerker.

1.2 Welke gegevens, van wie en waarvoor, staat in bijlage A.

1.3 Spreken onze algemene voorwaarden en deze overeenkomst elkaar tegen over persoonsgegevens, dan gaat deze overeenkomst voor.

2 Instructies

2.1 Wij verwerken de gegevens alleen op uw instructie. Uw instructies zijn de overeenkomst, de app zoals u die inricht en gebruikt, en wat u ons schriftelijk vraagt.

2.2 Wij gebruiken de gegevens niet voor eigen doeleinden.

2.3 Moeten wij op grond van Europees of Nederlands recht gegevens verwerken of verstrekken, dan melden we u dat vooraf, tenzij dat recht het verbiedt.

2.4 Is een instructie volgens ons in strijd met de AVG, dan melden we u dat direct.

3 Geheimhouding

3.1 Alleen wie het voor zijn werk nodig heeft, krijgt toegang tot de gegevens. Iedereen met toegang is tot geheimhouding verplicht.

4 Beveiliging

4.1 Wij nemen passende technische en organisatorische maatregelen om de gegevens te beveiligen. Bijlage C beschrijft ze.

4.2 Wij mogen de maatregelen aanpassen, zolang het beveiligingsniveau niet daalt.

4.3 U zorgt voor de beveiliging aan uw kant: wie toegang heeft tot de app, met welke rechten, en hoe tweestapsverificatie is ingesteld.

5 Subverwerkers

5.1 U geeft ons toestemming om de subverwerkers uit bijlage B in te schakelen.

5.2 Een nieuwe of andere subverwerker melden wij minstens 30 dagen vooraf per e-mail. Maakt u binnen die termijn bezwaar, dan zoeken we samen een oplossing. Lukt dat niet, dan mag u de overeenkomst voor de app waar het om gaat kosteloos opzeggen tegen de datum waarop de wijziging ingaat.

5.3 Elke subverwerker leggen wij dezelfde verplichtingen op als in deze overeenkomst staan. Wij blijven tegenover u verantwoordelijk voor hun werk.

5.4 Op uw verzoek geven wij informatie over onze subverwerkers en de afspraken met hen.

6 Doorgifte buiten de EER

6.1 Wij geven gegevens alleen door naar een land buiten de Europese Economische Ruimte met een waarborg uit de AVG, zoals een adequaatheidsbesluit of de standaardcontractbepalingen van de Europese Commissie. Bijlage B noemt per subverwerker waar de gegevens staan en welke waarborg geldt.

6.2 Vervalt een waarborg, dan stappen we over op een andere waarborg, of melden we u dat. U kunt dan bezwaar maken zoals in artikel 5.2.

7 Rechten van betrokkenen en hulp

7.1 Krijgen wij een verzoek van een betrokkene, zoals om inzage of verwijdering, dan sturen we het door naar u. Wij reageren er zelf niet inhoudelijk op.

7.2 De meeste verzoeken handelt u zelf af in de app. Is daar hulp van ons voor nodig, dan helpen wij.

7.3 Ook bij een DPIA of een vraag van de Autoriteit Persoonsgegevens helpen wij, met de informatie die wij hebben.

7.4 Hulp die meer vraagt dan een korte handeling, rekenen wij tegen ons uurtarief, tenzij de oorzaak bij ons ligt.

8 Datalekken

8.1 Ontdekken wij een datalek dat uw gegevens raakt, dan melden we dat zonder onredelijke vertraging aan uw contactpersoon, en uiterlijk binnen 48 uur.

8.2 In de melding staat wat er is gebeurd, welke gegevens en betrokkenen het raakt, wat de gevolgen kunnen zijn en wat we doen om ze te beperken. Weten we nog niet alles, dan vullen we de melding aan zodra we meer weten.

8.3 U beslist of het datalek gemeld wordt bij de Autoriteit Persoonsgegevens en bij betrokkenen. Wij melden het daar niet zelf.

8.4 Wij leggen elk datalek vast, met wat we eraan gedaan hebben.

9 Informatie en audit

9.1 Wij geven u de informatie die nodig is om te laten zien dat we ons aan deze overeenkomst houden. Dat doen we eerst met documentatie over onze beveiliging en met antwoorden op uw vragen.

9.2 Is dat niet genoeg, dan mag u eens per jaar een audit laten doen door een onafhankelijke auditor die tot geheimhouding verplicht is. U meldt de audit minstens 30 dagen vooraf, en de audit hindert ons werk niet meer dan nodig.

9.3 Na een datalek, of als de Autoriteit Persoonsgegevens erom vraagt, mag u ook tussentijds een audit laten doen.

9.4 De kosten van een audit zijn voor u, tenzij de audit een wezenlijke tekortkoming aan onze kant aantoont.

10 Einde

10.1 Deze overeenkomst loopt zolang wij persoonsgegevens voor u verwerken.

10.2 Na het einde kunt u een export van uw gegevens opvragen, zoals in artikel 13 van onze algemene voorwaarden staat. Daarna wissen wij de gegevens. Kopieën in onze back-ups zijn binnen vier maanden verwijderd. Het wissen bevestigen we per e-mail.

10.3 Moeten wij gegevens op grond van de wet langer bewaren, dan gebruiken we ze alleen daarvoor.

10.4 Afspraken die naar hun aard doorlopen, zoals geheimhouding, blijven na het einde gelden.

11 Aansprakelijkheid

11.1 Voor onze aansprakelijkheid gelden de beperkingen uit artikel 14 van onze algemene voorwaarden.

11.2 Een boete van een toezichthouder draagt de partij die de boete krijgt.

11.3 Spreekt een betrokkene of een toezichthouder ons aan omdat u gegevens onrechtmatig verwerkt of ons een onrechtmatige instructie geeft, dan vrijwaart u ons daarvoor.

12 Wijzigen en recht

12.1 Wij mogen deze overeenkomst wijzigen zoals artikel 18 van onze algemene voorwaarden beschrijft. Bijlage B wijzigen we volgens artikel 5, bijlage C volgens artikel 4.

12.2 Op deze overeenkomst is Nederlands recht van toepassing. Voor geschillen geldt artikel 19 van onze algemene voorwaarden.

Bijlage A De verwerking

Doel	Het bouwen, hosten, onderhouden en ondersteunen van de apps uit de overeenkomst.
Wat we doen	Opslaan en bewaren. Inzien bij support, herstel en onderhoud. Back-ups maken en terugzetten. E-mail en pushmeldingen versturen namens de app. Exporteren en wissen.
Betrokkenen	Afhankelijk van de app: uw medewerkers en andere gebruikers van de app, en uw klanten, leveranciers en andere relaties met hun contactpersonen.
Gegevens	Afhankelijk van de app: naam, e-mailadres, telefoonnummer, functie en rol. Inloggegevens en tweestapsverificatie, als hash of versleuteld. Wat in de app wordt vastgelegd, zoals uren, planning, werkzaamheden, adressen, offertes, notities, foto's, documenten en handtekeningen. Technische gegevens: IP-adres, tijdstippen van gebruik, de audit log en het pushadres van een toestel.
Niet bedoeld voor	Bijzondere persoonsgegevens, strafrechtelijke gegevens en het burgerservicenummer. Wilt u die toch verwerken, dan spreken we dat vooraf schriftelijk af.
Bewaren	Gegevens in de app: zolang u ze bewaart, tot het einde van de overeenkomst. Back-ups: 7 dagelijkse, 4 wekelijkse en 3 maandelijkse kopieën, plus snapshots volgens uw pakket. Foutmeldingen in onze monitoring: 14 dagen, met een HMAC van het e-mailadres in plaats van naam of e-mailadres. Pushadressen: tot de gebruiker zich afmeldt of de app 180 dagen niet gebruikt.
Waar	Op onze eigen servers in Nederland. Back-ups op eigen opslag in Nederland, buiten de servers van de app. Voor subverwerkers: bijlage B.

Bijlage B Subverwerkers

PARTIJ	WAARVOOR	WAAR	WAARBORG
Connectium B.V. Argonstraat 5, 7463 PD Rijssen	Beheer van de servers en het netwerk in de datacenters. De Microsoft 365-omgeving voor e-mail en bestanden van onze support. Medewerkers die meewerken aan bouw en support.	Nederland	Binnen de EER
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ierland	E-mail en bestanden van onze support, via de omgeving van Connectium.	EU Data Boundary	Binnen de EER; voor uitzonderingen het Data Privacy Framework
Brevo SAS 9-17 rue Salneuve, 75017 Parijs, Frankrijk	Versturen van e-mail uit de app, zoals uitnodigingen en wachtwoordherstel.	EU	Binnen de EER

PARTIJ	WAARVOOR	WAAR	WAARBORG
Google Ireland Limited Gordon House, Barrow Street, Dublin 4, Ierland	Pushmeldingen naar Android-toestellen, via Firebase Cloud Messaging.	Wereldwijd	Data Privacy Framework
Apple Distribution International Limited Hollyhill Industrial Estate, Hollyhill, Cork, Ierland	Pushmeldingen naar iPhone en iPad, via de Apple Push Notification service.	Wereldwijd	Standaardcontractbepalingen
Anthropic Ireland, Limited South Bank House, Barrow Street, Dublin 4, Ierland	AI in onze support en AI-functies in de app.	Verenigde Staten en wereldwijd	Standaardcontractbepalingen
Cloudflare, Inc. 101 Townsend Street, San Francisco, Verenigde Staten	Beveiliging van het verkeer naar ons supportportaal.	Wereldwijd	Data Privacy Framework

Bijlage C Beveiligingsmaatregelen

Hosting	Onze apps draaien op eigen servers in Nederland, verdeeld over drie datacenters. Elke omgeving van een app heeft een eigen database met een eigen wachtwoord, dat alleen die omgeving kent. Ontwikkeling, testomgeving en productie zijn gescheiden.
Toegang	Tweestapsverificatie staat standaard verplicht voor gebruikers van de app, met een authenticator-app, e-mailcode of passkey. Rechten gaan per rol. Wachtwoorden bewaren we als hash. Onze medewerkers krijgen alleen de toegang die ze voor hun werk nodig hebben, en onze sleutels staan in een wachtwoordmanager.
Versleuteling	Al het verkeer gaat over HTTPS, en dat wordt afgedwongen. Cookies zijn secure en samesite, en security headers staan aan. Het geheim van tweestapsverificatie slaan we versleuteld op.
Vastleggen	Wijzigingen aan gebruikers, rechten en klantgegevens komen in een audit log die niemand kan aanpassen of verwijderen.
Bewaking	Fouten en beschikbaarheid bewaken we dag en nacht. Een foutmelding bevat een HMAC van het e-mailadres in plaats van naam of e-mailadres, en wordt na 14 dagen verwijderd.
Back-up	Elke nacht een back-up naar aparte opslag in Nederland, buiten de servers van de app, plus snapshots volgens het pakket. Terugzetten kan naar het moment van een back-up of snapshot. Het terugzetten van een database is getest.
Ontwikkeling	Elke wijziging gaat via een pull request met automatische tests, eerst naar de testomgeving en dan naar productie. Een wijziging met een sleutel of wachtwoord in de code wordt tegengehouden. Gebruikte pakketten worden automatisch bijgewerkt, en kwetsbaarheden automatisch gesignaleerd.
Organisatie	Wij werken met een managementsysteem voor informatiebeveiliging volgens ISO 27001, samen met Connectium. Iedereen met toegang tot gegevens is tot geheimhouding verplicht.