

Zo beschermt DepotFlow jouw bedrijfsgegevens

Je vertrouwt DepotFlow met de kern van je bedrijf: je chauffeurs, je tarieven, je marges, je facturen. Dat vertrouwen verdienen we niet met mooie woorden, maar met hoe het systeem gebouwd is. Elke claim hieronder zit daadwerkelijk in de software.

■ ISOLATIE

**100%
gescheiden**

Elk bedrijf strikt afgeschermd, op elke aanvraag opnieuw gecontroleerd.

■ VERSLEUTELING

**AES-256
versleuteld**

BSN-gegevens op bankniveau, met de sleutel in een EU-kluis.

■ BACK-UPS

**Elke nacht
een back-up**

Offsite, 30 dagen onwijzigbaar en wekelijks automatisch getest.

■ INFRASTRUCTUUR

EU-hosting

Server, betalingen en back-ups blijven binnen Europa.

Kan een andere service partner bij mijn gegevens?

Nee. Dit is de eerste vraag die iedereen stelt, en de belangrijkste.

Elke keer dat je iets opvraagt, bepaalt het systeem op basis van je beveiligde sessie van welk bedrijf je bent. Die identiteit komt nooit uit iets wat je browser meestuurt en dat vervalst zou kunnen worden. Elke databasevraag wordt gefilterd op jouw bedrijf, en elk bestand (facturen, contracten, bonnetjes) staat in een aparte map per service partner met een controle die elke uitbraakpoging blokkeert.

Dit is niet alleen zo bedoeld, het is getest. We draaien automatische testen die proberen om vanuit het ene bedrijf de gegevens van een ander te zien. Die testen moeten falen voordat nieuwe software live mag. En het sluit ook ons eigen support af: kijkt een DepotFlow-medewerker mee om je te helpen, dan is dat altijd **alleen-lezen, maximaal vijftien minuten geldig, en volledig gelogd**. Kijken kan, wijzigen niet.



Identiteitscontrole op elke aanvraag

Het systeem leidt je identiteit af uit je beveiligde sessie, nooit uit je verzoek.



Service partner A

AFGESLOTEN



Jouw bedrijf

ALLEEN JIJ



Service partner C

AFGESLOTEN

Eén beveiligde database, strikt gescheiden per bedrijf. Jouw gegevens en die van een ander raken elkaar nooit, en die scheiding wordt op elke aanvraag opnieuw afgedwongen.

Wat als iemand mijn wachtwoord probeert te raden of te stelen?

Wachtwoorden worden nooit als leesbare tekst opgeslagen. Ze worden versleuteld met bcrypt, de standaard die ook banken gebruiken. Zelfs als iemand de database zou bemachtigen, is een wachtwoord daar niet uit terug te lezen.

Tegen raden zitten twee onafhankelijke sloten op de inlogpagina: te veel pogingen vanaf hetzelfde adres wordt geblokkeerd, en te veel mislukte pogingen tegen hetzelfde e-mailadres ook, zelfs als de aanvaller telkens van internetadres wisselt. Verlies je een telefoon waar je nog op ingelogd stond? **Eén wachtwoordwijziging sluit dat apparaat direct buiten**. Een herstellink is maar zestig minuten geldig, eenmalig te gebruiken, en versleuteld bewaard.

Worden mijn gevoelige gegevens versleuteld?

De meest gevoelige gegevens die we beheren zijn de BSN-nummers van chauffeurs in loondienst, nodig voor de loonadministratie. Die worden versleuteld opgeslagen met **AES-256, versleuteling op bankniveau**, waarbij de sleutel zelf veilig in de sleutelkluis van Google Cloud blijft, in een datacenter in Nederland (Eemshaven), en jaarlijks automatisch verversst wordt.

In het systeem zie je standaard alleen de laatste vier cijfers. Het volledige nummer wordt alleen ontcijferd op het ene moment dat het echt nodig is, de loonexport, en elke keer dat dat gebeurt wordt het vastgelegd. De software start in productie zelfs niet op als deze versleuteling niet correct staat ingesteld, juist om te voorkomen dat zulke gegevens ooit onversleuteld weggeschreven worden.

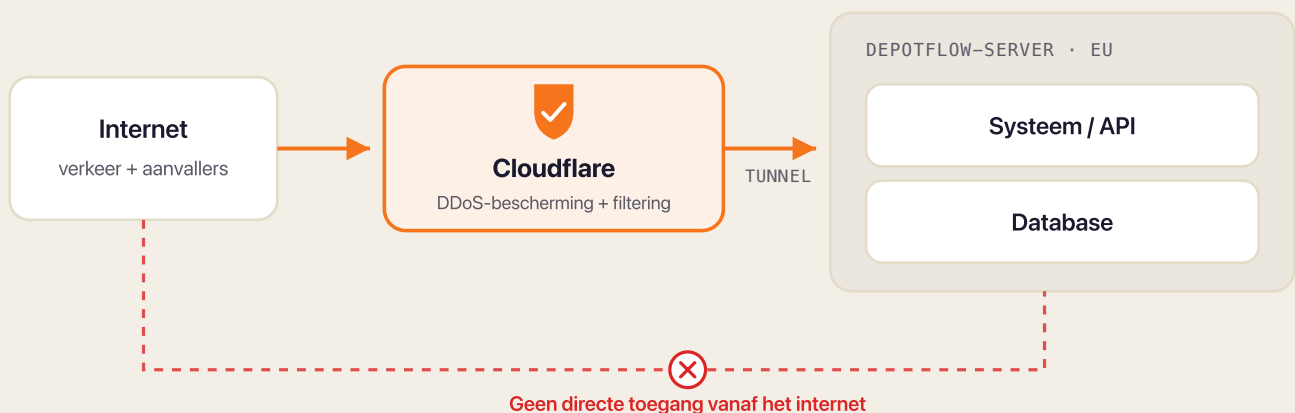


Versleuteld op bankniveau. Het slot en de sleutel zijn gescheiden: de sleutel ligt apart in een beveiligde kluis in Nederland, dus zelfs de versleutelde gegevens zijn zonder die kluis onleesbaar.

Wat als jullie server gehackt wordt of er data lekt?

DepotFlow draait op een server bij Hetzner in de Europese Unie. Het belangrijkste: **de systemen die jouw gegevens beheren staan niet open op het internet**. Al het verkeer loopt via het netwerk van Cloudflare, een van de grootste beveiligingsnetwerken ter wereld, dat aanvallen en overbelasting tegenhoudt voordat ze ons bereiken.

De database waar je gegevens in staan, en het systeem dat ze beheert, zijn niet rechtstreeks vanaf het internet bereikbaar. Verbindingen met de server zelf gaan alleen via versleutelde sleutel-toegang, wachtwoord-inloggen op de server is volledig uitgeschakeld, en een wachter blokkeert verdachte verbindingspogingen automatisch. Daarbovenop liggen lagen die fouten en aanvallen afvangen: bescherming tegen vervalste verzoeken, een strikte lijst toegestane adressen, limieten op uploads, en typecontrole op elk geüpload bestand.



Al het verkeer passeert eerst Cloudflare, dat aanvallen en overbelasting tegenhoudt. De server en de database zijn niet rechtstreeks vanaf het internet te bereiken — die deur bestaat simpelweg niet.

Wat als er iets kapotgaat? Ben ik mijn gegevens kwijt?

Elke nacht maakt het systeem een volledige back-up van de database en alle bestanden. Die wordt automatisch gecontroleerd op bruikbaarheid en daarna weggezet bij een tweede aanbieder in de EU, met een slot erop: **dertig dagen lang kan niemand die back-up wijzigen of verwijderen**, ook niet iemand die zich toegang tot de server zou verschaffen.

Het blijft niet bij hopen dat het werkt. Elke week zet het systeem automatisch een back-up terug in een aparte testomgeving en controleert of alles er nog is. Zou een back-up ook maar één nacht overslaan, dan krijgen we direct een melding. Er is een uitgeschreven herstelplan met als doel: maximaal één dag aan gegevens kwijt, volledig herstel in ongeveer een half uur.



Elke nacht een gecontroleerde back-up, onwijzigbaar bewaard in de EU, en elke week automatisch teruggezet om te bewijzen dat herstel echt werkt — niet alleen op papier.

Blijven mijn gegevens in Europa? Wie kan erbij?

De kern van je gegevens blijft in de EU: de server staat in de Europese Unie, betalingen lopen via Mollie in Nederland, en de back-ups staan in Europese opslag. Voor een paar ondersteunende diensten (het beveiligingsnetwerk en het versturen van e-mails) werken we met partijen met een hoofdkantoor in de VS. Dat doen we onder de wettelijk vereiste standaardcontractbepalingen, die jouw gegevens dezelfde bescherming geven.

We zijn open over precies welke partijen we inschakelen en waarvoor. De volledige lijst, met locatie en rol, staat in onze Verwerkersovereenkomst. Voegen we ooit een partij toe, dan melden we dat dertig dagen vooraf en kun je bezwaar maken.

Wat gebeurt er met betalingen?

DepotFlow ziet of bewaart nooit je kaartnummer of volledige bankgegevens. Het opzetten van een betaling gebeurt op de beveiligde pagina van Mollie. Wij bewaren alleen de verwijzing naar die betaling en de laatste vier cijfers van het rekeningnummer.

Betaal je je chauffeurs uit, dan verplaatst DepotFlow zelf geen geld. We maken een SEPA-bestand klaar dat jij in je eigen bank goedkeurt, met de inlog van je eigen bank. **Jij houdt de controle over elke euro die je rekening verlaat.**

Verzamelen jullie niet gewoon te veel?

Bewust niet. We slaan expres minder op dan zou kunnen. We bewaren geen kopieën van identiteitsbewijzen, omdat jij die als service partner zelf al wettelijk bewaart. Gegevens die alleen bij loondienst horen, kunnen bij zelfstandige chauffeurs simpelweg niet opgeslagen worden, dat blokkeert het systeem op meerdere niveaus. Chauffeurs hebben in hun eigen app een knop om hun gegevens op te vragen en hun account te laten verwijderen, en oude gegevens worden volgens vaste bewaartermijnen automatisch opgeruimd.

Hebben jullie dit door iemand laten controleren?

Ja, en het is geen eenmalige actie. Bij elke wijziging draait een vaste reeks controles: geautomatiseerde beveiligingsscan's, een aparte beveiligingsreview voor alles wat met inloggen, toegang of geld te maken heeft, en een controle op gevoelige gegevens. Code die deze controles niet doorstaat, gaat niet live.

Scheiding tussen bedrijven Op elk verzoek gecontroleerd, en automatisch getest

Versleuteling BSN op bankniveau, sleutel in een EU-kluis

Afgeschermd server Geen directe toegang vanaf internet, alles via Cloudflare

Back-ups Elke nacht, offsite, onwizigbaar, wekelijks getest

Betalingen Via Mollie, wij raken je bankgegevens niet aan

Privacy EU-hosting, minder verzamelen, volledig AVG-pakket

We claimen alleen wat er in zit

We zeggen niet dat DepotFlow onkwetsbaar is, dat zou niemand eerlijk kunnen zeggen. Wat we wel zeggen: beveiliging is hier geen vinkje achteraf, maar onderdeel van hoe er gebouwd wordt. Alles op deze pagina is iets wat daadwerkelijk in de software zit en is gecontroleerd, niet iets wat we nog van plan zijn.

Privacyverklaring

Welke gegevens we verwerken, hoe lang we ze bewaren, en jouw rechten.

Verwerkersovereenkomst (DPA)

De juridische afspraken, de volledige lijst ingeschakelde partijen, de datalekprocedure en je auditrechten.

Algemene Voorwaarden

De afspraken rond het gebruik van DepotFlow.

Vragen over beveiliging of je gegevens? Mail info@depotflow.nl.

DepotFlow is een product van PrimeSelects (KvK 94933898). Laatst bijgewerkt: 11 juni 2026.