FID Finance

Beveiligings-beleid

Hoe FID Finance B.V.
gegevens beveiligt

Versie	Partij	KvK	Btw-nummer
8 november 2026	FID Finance B.V.	80964303	NL861870293B01

FID Finance B.V.

Dit beveiligingsbeleid beschrijft de technische en organisatorische maatregelen waarmee FID Finance B.V. de gegevens van Opdrachtgevers en van zichzelf beschermt.

Handelsnamen	FID Finance & FID Controllers
Vestigingsadres	Havenweg 24, 4131 NM Vianen
E-mail	info@fidfinance.nl
Privacy	bart@fidfinance.nl
Telefoon	+31 34 774 8004
KvK-nummer	80964303
Btw-nummer	NL861870293B01
Bereikbaarheid	8:30 uur – 17:00 uur

Inhoud

Artikel 1	Doel
Artikel 2	Organisatie
Artikel 3	Werkplekken en accounts
Artikel 4	Het KPI-dashboard
Artikel 5	AI en koppelingen
Artikel 6	Leveranciers
Artikel 7	Incidenten
Artikel 8	Herziening

1 Doel

1. Dit beleid beschrijft hoe FID Finance de gegevens van Opdrachtgevers en van onszelf beveiligt: de technische en organisatorische maatregelen zoals de AVG (artikel 32) die vraagt. Het hoort bij de verwerkersovereenkomst (bijlage C).

2 Organisatie

1. De directie van FID Finance is verantwoordelijk voor de informatiebeveiliging.
2. Medewerkers hebben een geheimhoudingsplicht en krijgen alleen toegang tot wat ze voor hun werk nodig hebben.
3. Bij uitdiensttreding trekken we alle toegang direct in.
4. Medewerkers worden bewust gemaakt van risico's zoals phishing en het veilig gebruik van AI (zie ons AI-beleid).

3 Werkplekken en accounts

1. Onze ICT-partner Rijs ICT beheert en beveiligt onze Microsoft-omgeving (Microsoft 365, waaronder e-mail) en onze computers.
2. Een apparaat dat kwijt of gestolen is, kan op afstand worden geblokkeerd.
3. Persoonlijke accounts, geen gedeelde wachtwoorden; waar het kan met tweestapsverificatie.
4. Software en besturingssystemen houden we bijgewerkt.

4 Het KPI-dashboard

1. Hosting bij Railway in de EU-regio (Amsterdam); alle verbindingen versleuteld (HTTPS).
2. Per Opdrachtgever een eigen, afgeschermd deel van de database.
3. Persoonlijke accounts met rollen, tweestapsverificatie en bescherming tegen het raden van wachtwoorden.
4. Een logboek van wie wat wijzigde en wie inlogde.

5. De sleutels waarmee het dashboard de Odoo van een Opdrachtgever leest, staan versleuteld opgeslagen; het dashboard leest alleen en schrijft niets in Odoo.
6. Wachtwoorden worden nooit leesbaar bewaard.
7. Gegevens worden automatisch verwijderd volgens ons bewaarbeleid.

5 AI en koppelingen

1. AI werkt via onze eigen MCP-server met de Odoo van de Opdrachtgever; die bepaalt wat AI mag lezen en doen.
2. Toepassingen lezen alleen onderdelen van een vaste lijst, en alleen wat voor de taak nodig is.
3. Een mens keurt goed voordat er iets wordt geboekt of verzonden; per vraag houden we een audittrail bij.
4. AI-diensten alleen onder zakelijke voorwaarden zonder training op onze gegevens.

6 Leveranciers

1. Met leveranciers die voor ons persoonsgegevens verwerken, maken we de afspraken die de AVG vraagt. De actuele lijst staat in bijlage B van de verwerkersovereenkomst en op dashboard.fidfinance.nl/vertrouwen.

7 Incidenten

1. Een beveiligingsincident of datalek handelen we af volgens onze datalekprocedure. Elke medewerker meldt een (mogelijk) incident direct.

8 Herziening

1. We kijken dit beleid elk jaar na, en eerder bij een belangrijke wijziging in onze systemen of leveranciers.

Vragen over beveiliging?

Neem contact op via bart@fidfinance.nl, of via info@fidfinance.nl of +31 34 774 8004. Wij zijn bereikbaar van 8:30 tot 17:00 uur.

Supergoed in cijfers & mensen