



PalamedesAI

Information Security Policy (ISP)

Bij **PalamedesAI** begrijpen we dat financiële data de meest privacygevoelige informatie van uw organisatie en uw cliënten bevat. Onze software is ontwikkeld met een **Security-by-Design** filosofie. Dit betekent dat veiligheid geen achteraf-toevoeging is, maar de kern vormt van hoe onze applicatie technisch is opgebouwd.

Onderstaand vindt u onze belangrijkste waarborgen op het gebied van informatiebeveiliging.

1. Architectuur: Lokale Controle, Geen Cloudopslag

In tegenstelling tot veel moderne SaaS-oplossingen, werkt onze applicatie **lokaal (on-site)** binnen uw eigen infrastructuur.

- **In-Memory Processing:** Financiële data wordt uitsluitend in het werkgeheugen (RAM) van de lokale machine geladen tijdens de analyse.
- **Geen Persistente Opslag:** Wij bouwen geen database op met uw cliëntdata. Zodra het script wordt afgesloten, wordt het werkgeheugen volledig vrijgegeven en is er geen spoor van de verwerkte financiële data meer aanwezig op de lokale schijf of in onze cloud.
- **Stand-alone Werking:** De applicatie heeft geen permanente verbinding met onze servers nodig voor de verwerking van data.
- **Compliance:** deze werkwijze helpt ons te voldoen aan de **AVG (GDPR)** richtlijnen, omdat er geen sprake is van onnodige data-opslag.

2. Toegangsbeheer & Autorisatie

Wij hanteren het principe van '**Least Privilege Access**'. Onze A.I. Agent krijgt alleen toegang tot wat strikt noodzakelijk is.

- **OAuth2 Authenticatie:** De koppeling met Exact Online verloopt via de industrie standaard OAuth2, waarbij u zelf controle houdt over de toegang.
- **Read-Only Beperking:** De software heeft technisch **geen schrijfrechten**. De toegang is beperkt tot enkel het **lezen** van specifieke modules voor de jaarrekeningcontrole:
 - *GLAccounts* (Grootboekrekeningen)
 - *GLTransactionLines* (Mutaties)
 - *ReportingBalance* (Saldibalans)
- **Data Validatie:** Om foutieve koppelingen te voorkomen, valideert de software de cliënt-naam uit het opdrachtformulier met de API-respons van de administratie voordat de analyse start



PalamedesAI

3. Kunstmatige Intelligentie & Privacy

Voor de analyse maken wij gebruik van het **Google Vertex AI** platform. Wij hebben hierbij strikte afspraken gemaakt over de bescherming van uw data:

Aspect	Waarborg
Data Training	Uw data wordt niet gebruikt om de modellen van Google te trainen. De data blijft uw eigendom.
Enterprise Protection	Wij vallen onder de Google Cloud Enterprise Data Protection voorwaarden.
Encryptie in Transit	Alle communicatie met de AI-services vindt plaats via zwaar versleutelde verbindingen (TLS 1.2+).

4. Risicobeheer & Beveiliging van Sleutels

Zelfs in een lokale omgeving nemen wij maatregelen tegen ongeautoriseerde toegang:

- **Versleutelde Tokens:** De *Client Secrets* die nodig zijn voor de API-koppeling worden nooit als platte tekst opgeslagen. Deze zijn lokaal op de machine in versleutelde vorm aanwezig.
- **Voorkomen van Datalekken:** Doordat er geen centrale database bestaat waarin alle data van al onze klanten wordt verzameld, is het risico op een grootschalig datalek via ons platform technisch uitgesloten.

Onze belofte: Wij zien uw data nooit, wij slaan uw data niet op, en wij gebruiken uw data nooit voor andere doeleinden dan de directe analyse waarvoor u ons de opdracht geeft.

5. Contact

Voor vragen over ons Information Security Beleid kunt u contact opnemen met onze C.I.S.O. die beschikt over een certificaat CISSP en CISM.