

ProcessMind SaaS-hosting

Ingangsdatum: 14 september 2026

1. Inleiding

ProcessMind B.V. (“wij”, “ons”, “onze”) levert Software as a Service-oplossingen (SaaS) die worden gehost op de infrastructuur van Amazon Web Services (AWS) in **Frankfurt, Duitsland**. In dit hostingbeleid worden onze toezeggingen aan onze klanten en de normen volgens welke we werken uiteengezet, om de betrouwbaarheid, beveiliging en naleving van onze hostingomgeving te waarborgen.

2. Hostinginfrastructuur

Onze SaaS-oplossingen worden gehost op AWS, waarbij gebruik wordt gemaakt van de robuuste, schaalbare en veilige infrastructuur van Amazon Web Services. Het primaire datacenter voor onze diensten bevindt zich in Frankfurt, Duitsland, zodat je gegevens binnen de Europese Unie (EU) worden opgeslagen.

3. Gegevensbeveiliging

We zetten ons in om de beveiliging en integriteit van de gegevens van onze klanten te waarborgen. AWS biedt een zeer veilige omgeving met een uitgebreid pakket beveiligingsdiensten, waaronder:

- **Fysieke beveiliging:** De datacenters van AWS worden beschermd door uitgebreide fysieke beveiligingsmaatregelen om ongeoorloofde toegang te voorkomen.
- **Netwerkbeveiliging:** Firewalls, netwerkmonitoring en versleutelde communicatie beschermen gegevens tijdens verzending en in rust.
- **Toegangscontroles:** Er zijn strenge toegangscontroles en authenticatiemechanismen ingesteld om ervoor te zorgen dat alleen bevoegd personeel toegang heeft tot klantgegevens.

4. Gegevensprivacy

Je privacy is belangrijk voor ons. We voldoen aan alle relevante wetgeving inzake gegevensbescherming, waaronder de Algemene verordening gegevensbescherming (AVG). Raadpleeg ons [Privacybeleid](#) voor meer informatie over hoe we omgaan met je persoonsgegevens.

5. Beschikbaarheid van de dienst

We ontwerpen de productieomgeving met het oog op hoge beschikbaarheid door middel van redundantie, monitoring, gecontroleerde releases en operationele responsprocedures. Dit hostingbeleid is uitsluitend informatief en schept op zichzelf geen contractuele toezeggingen over de beschikbaarheid.

ProcessMind publiceert de actuele status, uptimepercentages en de geschiedenis van responstijden op processmind.com/status. De statuspagina wordt afzonderlijk van de frontend van de applicatie gehost; de actuele statusgegevens worden via onze API geleverd. Tijdens een API-incident blijft de pagina zelf dus beschikbaar, maar kan deze beperkte statusinformatie weergeven. Raadpleeg de [Service Level Agreement](#) voor informatie over de manier waarop de uptime wordt gemeten.

Contractuele toezeggingen over beschikbaarheid, doelstellingen voor incidentrespons, servicecredits en ondersteuningsvoorwaarden worden beschreven in de [Service Level Agreement](#).

6. Back-ups en herstel na calamiteiten

- **Back-ups:** Er worden ten minste dagelijks automatisch back-ups gemaakt van productieklantgegevens. Deze worden duurzaam opgeslagen binnen de AWS-regio; back-ups worden momenteel niet naar een tweede regio gerepliceerd.
- **Herstel na calamiteiten:** Herstelmaatregelen en prioriteiten worden beschreven in het overzicht van herstel na calamiteiten, bedrijfscontinuïteit en incidentrespons.

7. Naleving

ProcessMind wordt gehost op AWS-infrastructuur die over de volgende certificeringen beschikt:

- **ISO 27001**: management van informatiebeveiliging
- **ISO 27017**: cloudgerichte beheersmaatregelen
- **ISO 27018**: bescherming van persoonsgegevens in de cloud
- **SOC 1, SOC 2, SOC 3**: beheersmaatregelen voor serviceorganisaties

Deze certificeringen zijn van toepassing op de AWS-infrastructuur waarop ProcessMind actief is. ProcessMind neemt deze beheersmaatregelen over door gebruik te maken van door AWS beheerde diensten. ProcessMind heeft het traject gekozen voor de eigen ISO 27001-certificering en SOC 2 Type II-attestatie; het formele proces is nog niet gestart.

ProcessMind voldoet aan de Algemene verordening gegevensbescherming (AVG) op het gebied van gegevensbescherming en privacy. Raadpleeg het document [Beveiligingsmaatregelen](#) voor meer informatie over de eigen technische en organisatorische beveiligingsmaatregelen van ProcessMind.

8. Verantwoordelijkheden van de klant

Klanten zijn verantwoordelijk voor de beveiliging van hun accountgegevens en voor alle handelingen die met hun accounts worden verricht. Klanten dienen:

- Sterke, unieke wachtwoorden voor hun accounts te gebruiken.
- Waar beschikbaar multifactorauthenticatie (MFA) te gebruiken.
- Toegangsrechten regelmatig bij te werken en te controleren.
- Verdachte activiteiten of beveiligingsinbreuken onmiddellijk aan ons ondersteuningsteam te melden.

9. Wijzigingen in het hostingbeleid

We kunnen dit hostingbeleid van tijd tot tijd bijwerken om wijzigingen in onze werkwijzen of wettelijke vereisten weer te geven. We stellen klanten via onze website of rechtstreeks op de hoogte van wezenlijke wijzigingen.

Gerelateerd beleid

Raadpleeg de Service Level Agreement voor informatie over het indienen van ondersteuningsverzoeken, de prioritering van verzoeken en contractuele toezeggingen.

Contactgegevens

Neem bij vragen of opmerkingen over dit hostingbeleid contact met ons op via:

ProcessMind B.V.

Willem Sandbergstraat 33,
7425RC, Deventer,
Nederland

Telefoon: +31 85 060 68 09

E-mail: support@processmind.com

Door onze diensten te gebruiken, bevestig je dat je dit hostingbeleid hebt gelezen. Het wordt uitsluitend ter informatie verstrekt en schept geen contractuele verplichtingen naast de verplichtingen in de Klantovereenkomst, de Gegevensverwerkingsovereenkomst, de Service Level Agreement en de Beveiligingsmaatregelen.