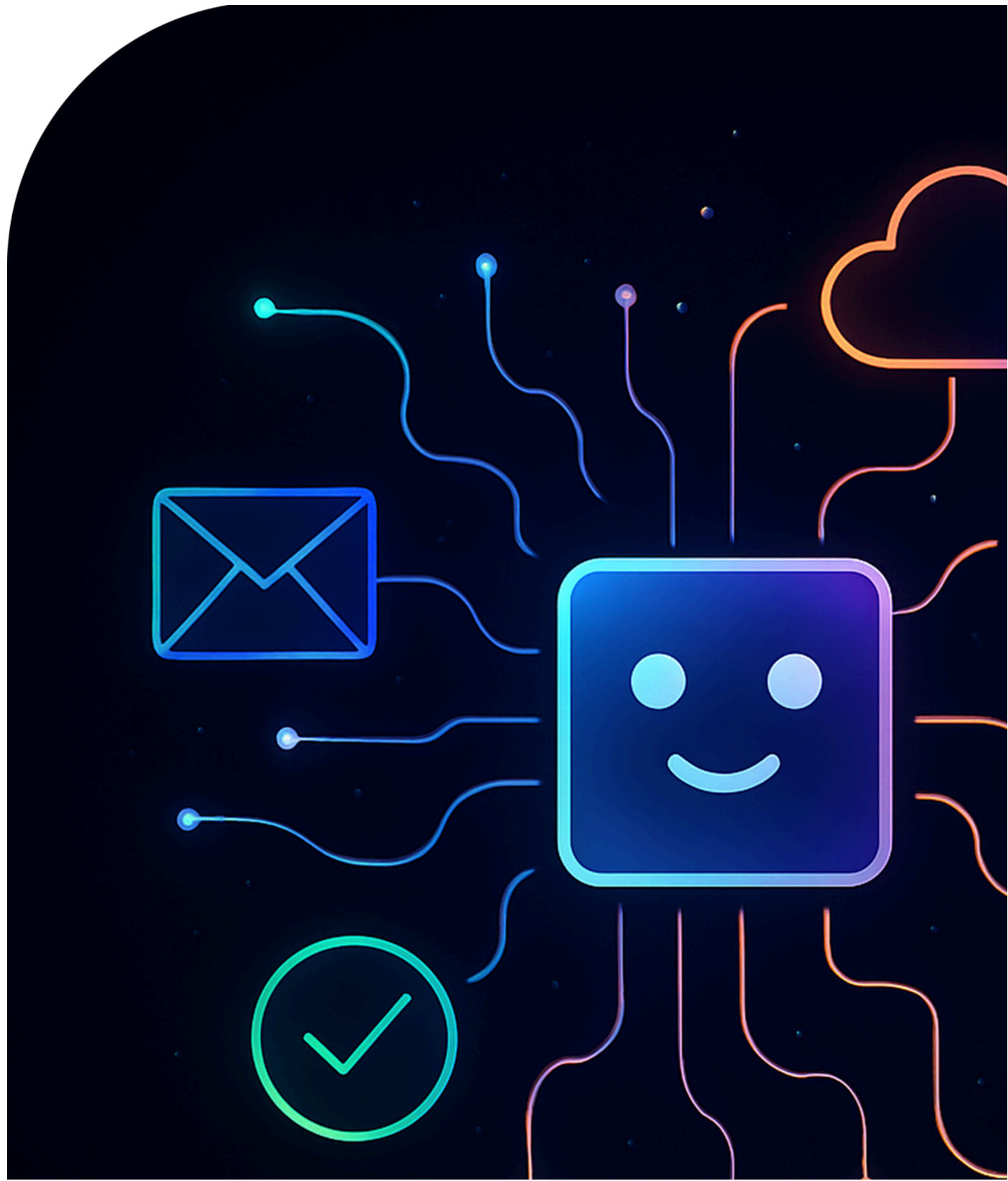


AI Agents bouwen met het Grexx Platform

Technische achtergrond



Inhoudsopgave

• Een kijkje onder de motorkap van het Grexx Digitalization Platform	3
• Over het Grexx Platform	4
○ Low Code Digitaliseringsplatform	4
○ Waarom is AI en low code een logische combinatie?	4
○ Dieper in de Grexx architectuur: álles is een case	5
○ Wisselen tussen AI en regelgebaseerde toepassing	6
○ Human-in-the-loop (HITL)	6
• Innovatie	7
○ Vrijheid in modellen in veilige eigen omgeving	7
○ Altijd de best passende optie: gemakkelijk wisselen tussen modellen	8
• Randvoorwaarden: compliance & governance	9
○ Audit trail	9
○ Metrics	9
○ Governance	9
○ Configureerbare bouwsteen	10
○ Compliance	11
• Impact maken	12
• Neem contact met ons op	13
○ Liever even spreken?	13

Een kijkje onder de motorkap van het Grexx Digitalization Platform

In dit document beantwoorden we een aantal veelgestelde vragen rondom de techniek achter ons low code platform. We behandelen onder andere de architectuur, het kiezen en hosten van taalmodellen en je mogelijkheden zijn qua rechtenstructuur en governance.

Natuurlijk zijn er nog veel meer (technische) zaken die we je zouden kunnen vertellen over het zelf ontwikkelen van AI Agents op ons platform. Heb je vragen of wil je eens zien hoe een en ander werkt, neem dan gerust contact met ons op. We denken graag mee over wat jouw organisatie nodig heeft en of het Grexx Platform dat kan bieden.

Je kunt [rechtstreeks een demo inplannen](#), of neem contact met ons op via [035 – 548 65 45](tel:035-5486545). Liever zelf rondkijken? [Meld je aan voor een free trial](#)

Hoe zat het ook alweer met AI, Generatieve AI en AI Agents?

AI, artificial intelligence en kunstmatige intelligentie zijn overkoepelende termen voor verschillende vormen van machine learning en intelligente automatisering.

Generatieve AI, ook wel *Gen AI*, is één van die vormen van AI. Generatieve AI genereert nieuwe content op basis van een menselijke instructie of 'prompt'. Het bekendste voorbeeld is hoe ChatGPT antwoorden formuleert op gebruikersvragen, op basis van de data waarmee het getraind is. Andere bekende voorbeelden van Gen AI zijn Google Gemini en Microsoft Copilot.

De **output** die Gen AI genereert kan verschillende vormen hebben: een tekst, een afbeelding, video of geluid. Wat Gen AI genereert is afhankelijk van wat de gebruiker vraagt (het prompt) in combinatie met de data waarmee het taalmodel getraind is. Dat kan van alles zijn, denk bijvoorbeeld aan openbaar beschikbare informatie op internet, wetenschappelijke publicaties of de database van Wikipedia. Of meer zakelijk toepasbaar: de handleidingen van jouw producten of de inbox van je klantenservice.

Wie aan de slag gaat met AI, werkt doorgaans met een **AI-agent**: een software-systeem dat met behulp van AI kan redeneren en acteren. De output is in dat geval vaak tekst (zoals een antwoord op een vraag aan de klantenservice) of een handeling (zoals een wijziging in de orderstatus na een data-analyse). Met het Grexx Platform kun je zelf AI-agents ontwikkelen die (delen van) je bedrijfsprocessen kunnen overnemen, versnellen en verslimmen, met een beperkte of zonder menselijke tussenkomst. In dit whitepaper lees je wat meer over de techniek die daar achterzit.

Over het Grexx Platform

Low Code Digitaliseringsplatform

Bij Grexx bieden we je een low code platform als fundament voor jouw digitalisering. Met ons platform bouw je flexibele maatwerksoftware die precies doet wat jouw organisatie nodig heeft – met AI of zonder AI, wat je wil. Groot voordeel van low code is dat het zeer flexibel en schaalbaar is, én dat je geen programmeerkennis nodig hebt.

Je kunt ons platform zien als een grote toolbox vol bouwblockjes die je kunt inzetten om jouw bedrijfsprocessen te digitaliseren en automatiseren. Die bouwblockjes zijn visueel van aard en iedere kenniswerker kan er mee aan de slag. Onder onze gebruikers vind je zowel programmeurs als niet-IT'ers: wat je nodig hebt is analytisch denkvermogen en kennis van de processen binnen het bedrijf. Programmeerkennis kan soms helpen, maar is geen vereiste. Ons team helpt jouw organisatie aan de juiste kennis en vaardigheden om zélf te bouwen.

Low code is een hele fijne optie voor digitale transformatie, vanwege de snelle prototypes, snelle aanpassingen en snelle implementaties. Omdat je zelf aan de knoppen zit en bestaande stukken techniek gebruikt kun je direct reageren op gebruikersfeedback of ontwikkelingen in de markt. Dat maakt low code flexibel en schaalbaar, en ideaal om in te zetten in experimenteren en doorontwikkelen met AI.

Waarom is AI en low code een logische combinatie?

Low code leent zich heel goed om bedrijfsprocessen efficiënt te digitaliseren, zonder uitgebreide programmeerkennis. Voeg je daar AI aan toe, dan kun je je processen niet alleen automatiseren maar ook slimmer maken: AI agents kunnen context begrijpen, patronen herkennen en proactief acties uitvoeren.

Sinds een paar jaar geleden ChatGPT het grote publiek wist te bereiken, zijn we collectief onder de indruk. We zien hoeveel tijd en energie AI ons kan besparen en hoe groot de mogelijkheden zijn. Diezelfde mogelijkheden werken ook verlamdend: als alles kan, waar begin je dan? Heel simpel: met een klein stukje. Je probeert iets, op kleine schaal, en afhankelijk van de resultaten stuur je bij of breid je uit. Zo doe je ervaring op met AI, leer je wat werkt voor jouw organisatie én wat problemen oplevert. Verantwoord en gecontroleerd.

Omdat low code snel en eenvoudig bij te sturen is, biedt het je de ideale proeftuin voor experimenteren, oefenen en testen met AI.

Dieper in de Grexx architectuur: álles is een case

Het Grexx Platform biedt een unieke case-based architectuur, een opzet die het mogelijk maakt om *alles* met *alles* te verbinden. We gaan daarin vaak heel ver en beschouwen alles in onze applicatiemodellen waar we "de" aan kunnen toevoegen als een case. Niet alleen "order", "klant" of "voorraadartikel" in de applicaties van onze klanten, maar ook "gebruiker", "homepage" of "menu-item". Oftewel, *alles is een case*.

Dat heeft veel voordelen, waaronder extreme flexibiliteit. Je hoeft niet te kiezen tussen objectgeoriënteerd, servicegeoriënteerd of een andere traditionele oriëntatie. De case-oriëntatie combineert de voordelen en behoudt overzicht, vooral in het digitaliseren van complexere processen.

Een case is onze weergave van de combinatie van de volgende elementen:

- Een object
- Een (cloud) GUI
- Een uitgebreid model voor rolgebaseerd toegangscontrole (RBAC)
- Een audit trail
- Een interface

Omdat elke case een object is, heeft het velden (we noemen ze attributen), methoden (activiteiten) en een definitie van de klasse (casetype), waardoor het mogelijk is om meerdere cases van hetzelfde casetype te aggregeren. Omdat elke case een GUI heeft, kun je de case via internet bereiken via de gewone browser. In de casetype-definitie definieer je weergaven en widgets die de GUI van de case vormen en definieer je wat gebruikers kunnen zien en waarmee ze kunnen interacteren wanneer ze een case bekijken.

Meer weten over onze architectuur en casebasedoriëntatie? Lees ons [whitepaper over architectuur](#) of [plan een demo](#) met een van onze collega's.

Wisselen tussen AI en regelgebaseerde toepassing

De inzet van AI agents is handig, maar niet altijd de beste oplossing voor jouw processen. Soms wil je gewoon regelgebaseerd werken. Bijvoorbeeld omdat op actie A altijd actie B volgt. Of omdat je duurzamer of sneller wil werken. En dat kan natuurlijk: met ons low code platform is dat helemaal geen probleem. Je kunt je processen eenvoudig regelgebaseerd opbouwen en combineren met AI, of andersom.

En wil je na verloop van tijd een deel van het proces anders invullen, dan kun je dat eenvoudig wijzigen. Vaak enkel door diezelfde *low code bouwblokjes* anders in te stellen, zonder dat je het hele proces opnieuw hoeft te digitaliseren.

Human-in-the-loop (HITL)

Indien gewenst is het altijd mogelijk om human-in-the-loop mogelijk te maken, om zo AI en menselijk handelen eenvoudig te combineren. Zo houden menselijke collega's altijd de controle over een proces.

Je kunt voor iedere AI agent die je bouwt tot op detailniveau aangeven welke rechten van toepassing zijn. Een belangrijke distictie hierin is *execute* of *suggest*. *Execute* betekent dat de AI agent volledig autonoom een function call kan doen. *Suggest* betekent dat de AI agent een function call klaarzet, waarbij de 'human-in-the-loop' zelf op submit drukt na het controleren van de inhoud.

Wil je de human-in-the-loop na verloop van tijd uit het proces halen? Dan kun je dat met één vinkje aanpassen. Zo kun je stapsgewijs toewerken naar het geleidelijk overdragen van taken aan een AI agent.

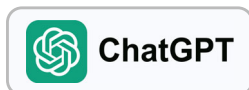
Innovatie

De ontwikkelingen in AI gaan razendsnel. Wat vandaag kan was vorig jaar ondenkbaar. En wat volgend jaar kan, dat kunnen we ons nu nog nauwelijks voorstellen. Met het Grexx Platform houd je jouw opties open. Wij zorgen ervoor dat je toegang hebt tot de 'best of breed' van beschikbare AI-technologie. Nu, en in de toekomst. Daarnaast kun je altijd bij ons terecht voor advies rondom verschillende modellen en technieken. We adviseren en denken graag mee wat bij jouw doelstellingen past.

Vrijheid in modellen in veilige eigen omgeving

Ga je met het Grexx Platform aan de slag, dan krijg je out of the box krijg je beschikking over een aantal publieke modellen die Grexx voor je beheert:

- **Externe modellen**



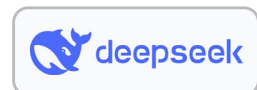
By OpenAI



By Google

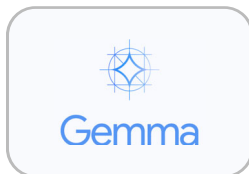


By Anthropic

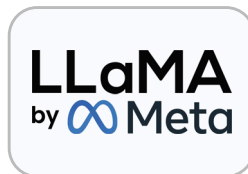


By High-Flyer

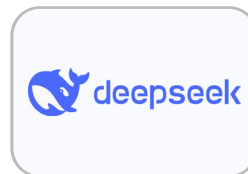
- **En lokale modellen**



By Google



By Meta



By High-Flyer

Daarnaast kun je ook **eigen modellen** configureren. Je kunt bijvoorbeeld met een eigen key gebruikmaken van een externe provider of een custom model bij OpenAI.

Binnen het Grexx Platform bieden we de mogelijkheid om (delen van) deze modellen te draaien op onze omgeving, op een eigen server die afgeschermd is van de buitenwereld. Het is ook mogelijk om deze modellen te hosten op een eigen server of datacentrum binnen de infrastructuur van de organisatie. We adviseren en denken graag met je mee over de gewenste opties met het oog op dataveiligheid en cybersecurity.

Maak je gebruik van een van de publieke modellen dan kun je de billing via Grexx laten lopen, of zelf een abonnement aanschaffen en dat koppelen aan je Grexx-omgeving.

Altijd de best passende optie: gemakkelijk wisselen tussen modellen

Zoals altijd in IT is er geen échte 'beste oplossing'. En wat vandaag perfect past, kan morgen misschien beter anders ingevuld worden. Idealiter verbind je je dus niet aan één specifieke aanbieder of model. Met het Grexx Platform heb je die flexibiliteit. Zo kun je eenvoudig wisselen tussen verschillende taalmodellen. Omdat een bepaald model beter past bij wat je nodig hebt, of gewoon omdat je eens wil proberen wat de resultaten zouden zijn. Met een paar kliks is het geregeld. En... bevalt het niet? Dan kun je net zo gemakkelijk weer terug.



Randvoorwaarden: compliance & governance



Audit trail

Je wil te allen tijde weten wat er gebeurt binnen je processen. Binnen je Grexx-omgeving is dat uiteraard goed inzichtelijk. Je houdt eenvoudig toezicht op AI agents via de bestaande audit-trail, aangevuld met extra inzichten in de (eventuele) beslissingen die door AI agents zijn genomen. Dit biedt een duidelijk overzicht van alle door de AI agents uitgevoerde activiteiten, met vermelding van betreffende AI agent en mogelijkheid tot doorklikken naar specifieke thread waarin een beslissing genomen is.

Ook extra inzichten (reasoning) rondom genomen beslissingen zijn hier terug te vinden. Zo bieden we transparantie en traceerbaarheid binnen het platform.

Metrics

Worden orders vaker succesvol afgerond? Zijn klanten meer of minder tevreden? Worden helpdeskvragen sneller afgehandeld? Dit soort vragen wil je na inzet van een AI agent kunnen beantwoorden. Daarvoor biedt het Grexx Platform een dashboard waarop je KPI's geautomatiseerd kunt bijhouden. Zodat de toegevoegde waarde van je applicatie eenvoudig onderbouwd kan worden.

Governance

Een van de grootste zorgen rondom AI is het vertrouwen: mag een AI agent zomaar alle beschikbare data en functionaliteiten gebruiken? Het is verleidelijk om AI agents aan alle mogelijke systemen te koppelen, want er zijn zó veel mogelijkheden en al die kansen benutten we graag. Maar... Veel AI-projecten creëren zo een oncontroleerbare *black box*, waarin (met én zonder AI) te veel tegelijk gebeurt, dat niet goed traceerbaar is én onvoldoende begeleid wordt. Wat ons betreft is risicobeheersing een grote succesfactor in werken met AI. En dat pakken we dus anders aan.

Het Grexx Platform biedt een zeer flexibele rechtenstructuur, die je zo specifiek kunt maken als je zelf wilt. Je kunt AI agents op verschillende manieren rechten toewijzen, bijvoorbeeld in lijn met wat bepaalde medewerkers mogen of gekoppeld aan welke systemen op bepaalde processen relevant zijn. Je kunt - indien gewenst - op detailniveau aangeven welke rechten bij welke taken horen, en welke beperkingen AI agents kennen.

Een voorbeeld uit de praktijk: We zitten op de klantenservice van een internetprovider. Een AI agent behandelt een salesvraag van een klant. De AI agent kan op dat moment geen

klantdata van andere klanten bekijken en ook geen wijzigingen doen aan de status van andere orders. En de AI agent kan tijdens het behandelen van een salesvraag ook niet in het systeem waarmee de router van de klant gereset wordt. We zorgen ervoor dat de AI agent alleen de op dat moment relevante rechten heeft, om de kans op fouten te beperken.

Door het inperken van rechten en goed na te denken over de structuur daarin, voorkomen we hallucinaties en verkeerde interpretaties. Een gebrek aan dat soort controle is de belangrijkste reden dan een groot deel van de AI-projecten faalt: er gebeurt te veel tegelijk, en er is niet geanticipeerd op wat AI fout doet. Dat AI fouten maakt is gegarandeerd, het is aan de gebruiker ervan om daarop voor te sorteren. Blind vertrouwen is nog niet mogelijk (en ook niet nodig!).

Configureerbare bouwsteen

Zo'n oncontroleerbare black box willen we dus voorkomen. In plaats daarvan bieden we een configureerbare bouwsteen. Een bouwsteen waarin je tot op de kleinste details rechten kunt toewijzen en beperken, en die ook precies laat zien wat er allemaal gebeurt. Je hebt altijd 100% toezicht op AI agents via de audit-trail binnen het Grexx Platform, aangevuld met extra inzichten en beslissingen die door AI agents zijn genomen.

Het toewijzen van de juiste rollen is eenvoudig en overzichtelijk. Dit kan taak-gerelateerd zijn: AI agents die zich met salesvragen bezighouden, krijgen deze rechten, AI agents die op de helpdesk zitten krijgen andere rechten. Rechten kunnen ook indirect toegewezen worden, bijvoorbeeld wanneer vanuit de AI agent vanuit proces A doorstroomt naar proces D en daar andere rechten voor nodig heeft.

Je kunt ook kiezen voor een 'human-in-the-loop' aanpak, waarbij een menselijke collega altijd de doorslag geeft: AI Agents krijgen dan wél allerlei rechten om zaken uit te zoeken, voor te bereiden en klaar te zetten, maar het is vervolgens een mens dat op enter moet drukken voor akkoord.

Verder kun je ervoor kiezen of AI agents elkaar mogen activeren, of zelf allerlei maatwerkopties ontwikkelen die perfect passen bij hoe jouw bedrijfsprocessen in elkaar zitten. Binnen de low code toolbox is veel mogelijk en we denken altijd graag met je mee over de invulling hiervan.

Compliance

Omdat het Grexx Platform zo strak configureerbaar is, passen jouw applicaties perfect binnen de bestaande wet- en regelgeving. Binnen het Grexx Platform bieden we de mogelijkheid om (delen van) de modellen die je gebruikt te draaien op onze omgeving, op een eigen server die afgeschermd is van de buitenwereld. Het is ook mogelijk om deze modellen te hosten op een eigen server of datacentrum binnen de infrastructuur van de organisatie. We adviseren en denken graag met je mee over de gewenste opties met het oog op dataveiligheid en cybersecurity.

Goed om te weten: Grexx is **ISO 27001** en **NEN 7510** gecertificeerd. Daarnaast hanteren we een **SOC2 ISAE 3000 Type II assurance report** en zijn we uiteraard **AVG-compliant**. De beschikbaarheid, integriteit en vertrouwelijkheid van het Grexx Platform laten we jaarlijks testen door externe auditors. Security en dataveiligheid nemen we zeer serieus, zowel voor onszelf als onze klanten. Je ziet dit onder andere terug in de governance-structuur die het platform biedt. We zijn je meer dan graag van dienst om daar optimaal gebruik van te maken.

Impact maken

Impact maken met technologie, of het nu gaat om 'gewoon' applicaties bouwen of specifiek de inzet van AI, start altijd met een paar kleine stappen. Proberen wat voor je werkt, ervaring opdoen, de eerste successen boeken en door blijven ontwikkelen.

Ben je eenmaal op stoom, dan maak je steeds sneller grote stappen. Met inzet van het Grexx Platform is dat ook zo. Ons Platform is laagdrempelig in te zetten en zo low code mogelijk. Zowel technisch onderlegde medewerkers als 'gewone' kenniswerkers kunnen er snel mee uit de voeten, ook omdat we flink investeren in coaching en training. We horen zeer regelmatig dat gebruikers veel sneller dan verwacht écht aan de slag kunnen, en daar zijn we trots op.

Heb je de eerste bedrijfsprocessen op ons Platform gedigitaliseerd en eventueel geautomatiseerd? Dan treedt een hefboom in werking: het wordt steeds gemakkelijker om nieuwe processen op te pakken, omdat de al aanwezige kennis over je bedrijf steeds toeneemt.

Ons Platform is sterk gericht op hergebruik en efficiënte inzet van bestaande informatie. Dat doen we met de configureerbare bouwsteentjes: gebruik vooral opnieuw, poog niet steeds het wiel opnieuw uit te vinden. Ook de uitgebreide integratiemogelijkheden en de marketplace dragen bij aan deze gedachte: je kunt eenvoudig bestaande functionaliteiten of prompts toevoegen aan je eigen applicatie.

Hoe meer projecten je met het Grexx Platform digitaliseert en automatiseert, hoe meer AI agents je bouwt, hoe beter en sneller je volgende project zal verlopen. De tijd die je nodig hebt om iets nieuws te bouwen neemt daarmee snel af.

Neem contact met ons op

Ben je benieuwd of het Grexx Digitalization Platform past bij wat jouw organisatie nodig heeft? Plan dan een [discovery call](#). We denken graag met je mee en dan laten we je direct zien wat mogelijk is. Liever zelf aan de slag? [Meld je aan voor een free trial](#).

Liever even spreken?

Neem contact met ons op via [035 – 548 65 45](tel:035-5486545) of info@grexx.net.