uniserver

Voldoe met Private AI aan de eisen van de EU

E-book

Inhoud.

Introductie.

AI wordt steeds belangrijker voor moderne bedrijven. Het helpt bij efficiënter werken, een betere klantbeleving en om gepersonaliseerde diensten aan te kunnen bieden. AI kan enorme hoeveelheden data analyseren en inzichten genereren die je helpen bij het nemen van betere strategische beslissingen, het automatiseren en optimaliseren van processen en het verbeteren van producten of diensten. Maar de opkomst van AI brengt ook nieuwe uitdagingen met zich mee, vooral op het gebied van (data)privacy. Juist door de grote hoeveelheden persoonlijke of gevoelige data die nodig zijn om effectief te kunnen werken. Dit vergroot het risico dat deze data verkeerd wordt gebruikt of in verkeerde handen valt. Maar hoe ga je daar dan goed mee om?

Waarom dit e-book?

Met dit e-book willen we je informeren over de impact die de GDPR (General Data Protection Regulation) en de EU AI Act hebben op het gebruik van AI-technologieën. Daarnaast laten we je zien hoe je met onze Private AI-dienst gemakkelijk kunt voldoen aan de eisen en toch gebruik kunt maken van de nieuwste innovatieve ontwikkelingen op het gebied van AI.

Het ontstaan van de GDPR.

Zorgen over de bescherming van de privacy van consumenten, de naleving van wetgeving en de ethische implicaties van datagebruik heeft geleid tot de GDPR die sinds 25 mei 2018 van kracht is. Deze wetgeving zorgt ervoor dat organisaties verantwoordelijk worden gehouden voor de manier waarop zij persoonsgegevens verzamelen, opslaan en verwerken.

De GDPR legt strikte verplichtingen op en stelt met name deze eisen:

- Organisaties moeten expliciete toestemming verkrijgen van individuen voordat zij hun persoonsgegevens verzamelen of verwerken.
- Persoonsgegevens mogen alleen verzameld worden als ze relevant en noodzakelijk zijn voor het specifieke doel waarvoor ze worden verzameld. Er moet een beperking zijn op de hoeveelheid data die verzameld wordt.
- Organisaties moeten de betrokkenen duidelijk informeren over de verwerking van hun persoonsgegevens, inclusief de doeleinden, de juridische basis voor de verwerking, de betrokkenen en hun rechten.
- Individuen hebben het recht om hun persoonsgegevens te laten wissen wanneer deze niet meer nodig zijn voor de doeleinden waarvoor ze verzameld zijn of wanneer ze hun toestemming intrekken.
- Betrokkenen hebben het recht om hun persoonsgegevens in te zien, te corrigeren of bij te werken.
- Betrokkenen hebben het recht om zich te verzetten tegen geautomatiseerde besluiten die hen juridisch raken of hen op negatieve wijze beïnvloeden, tenzij er expliciete toestemming is of het noodzakelijk is voor een contract.

De combinatie GDPR en EU AI Act: een compleet raamwerk.

Naast de GDPR, is in augustus 2024 de EU AI Act in werking getreden. Deze verordening bestaat uit regels die specifiek gelden voor het gebruik van AI-systemen in alle landen van de Europese Unie.

De kernpunten uit de EU AI Act zijn:

- Een op risico's gebaseerde benadering: AI-systemen worden ingedeeld op basis van risiconiveau - van minimaal tot onaanvaardbaar.
- Verbod op gevaarlijke AI: AI-systemen die de rechten en veiligheid van mensen ernstig in gevaar brengen zijn verboden, ook voor overheden.
- Strenge eisen voor hoog risico-AI: AI-toepassingen in gevoelige domeinen zoals gezondheid, recht en onderwijs moeten aan strikte voorwaarden voldoen.
- Transparantie-eisen: gebruikers moeten weten wanneer ze met AI te maken hebben.
- Toezicht en boetes: nationale en EU-autoriteiten controleren de naleving en kunnen zware financiële sancties opleggen die tot in de tientallen miljoenen euro's kunnen lopen.

Voor AI-toepassingen die persoonsgegevens verwerken, moeten organisaties voldoen aan beide regelgevingen, wat betekent dat ze zowel de bescherming van persoonsgegevens moeten waarborgen (GDPR) als de risico's en veiligheid van het AI-systeem zelf (AI Act) goed moeten beheren. Samen vormen de AI Act en de GDPR dus een compleet raamwerk dat privacy, veiligheid en ethiek van AI-gebruik binnen de EU waarborgt.

Waarom AI-systemen extra gevoelig zijn voor misbruik en non-compliance.

AI-systemen verwerken vaak op grootschalige wijze persoonsgegevens, wat de kans vergroot dat persoonlijke gegevens onzorgvuldig worden behandeld. Doordat ze gegevens verzamelen uit verschillende bronnen, wordt het beheer van de toestemming van betrokken personen zeer complex. Bovendien kan AI geautomatiseerde beslissingen maken zonder menselijke tussenkomst. De GDPR stelt dat individuen het recht hebben om niet onderworpen te worden aan puur geautomatiseerde besluitvorming, tenzij daar een juridische basis voor is.

GDPR en AI – Wat je moet weten

AI-systemen brengen specifieke uitdagingen met zich mee binnen de GDPR:

Recht op menselijke tussenkomst (Artikel 22)
Personen mogen niet uitsluitend onderworpen worden aan geautomatiseerde besluitvorming zonder menselijke controle, tenzij dit juridisch of contractueel noodzakelijk is, of met expliciete toestemming.

Transparantie
Organisaties moeten uitleggen hoe AI werkt, welke data wordt gebruikt, en hoe uitkomsten worden gecontroleerd.

Toestemmingsbeheer
Het verzamelen van data uit meerdere bronnen maakt het complex om toestemming correct te beheren. Zorg voor duidelijke systemen om naleving te waarborgen.

Data-minimalisatie
AI mag alleen noodzakelijke gegevens verwerken en moet sterk beveiligd zijn tegen misbruik.

Veel voorkomende fouten bij gebruik van AI.

Organisaties maken, vaak onbedoeld en onbewust, fouten bij het gebruik van AI die juridische, financiële en imagoschade tot gevolg kunnen hebben. Zij maken bijvoorbeeld gebruik van publieke AI-systemen zonder inzicht te hebben in waar hun data naar toe gaat en hoe deze wordt verwerkt. Dit kan leiden tot ongeautoriseerde toegang of schendingen van de GDPR. Soms kunnen AI-systemen zelfs persoonsgegevens verwerken op manieren die niet voldoen aan de wetgeving. Door bijvoorbeeld gegevens op te slaan in internationale datacenters zonder beveiligingsmaatregelen en privacy garanties.

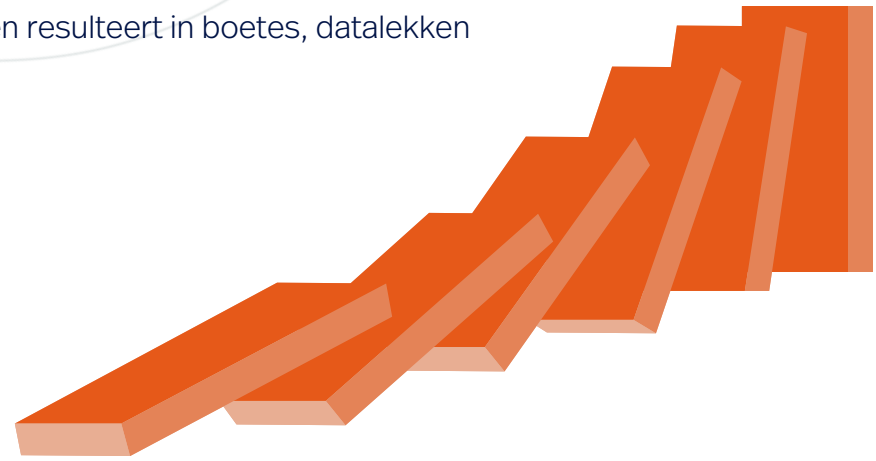
Het domino-effect van AI-fouten

Gebrek aan inzicht in dataverwerking
Organisaties gebruiken publieke AI-systemen zonder te weten waar data terecht komt.

Dataverwerking zonder controle
Persoonsgegevens worden verwerkt zonder duidelijke toestemming of controle, wat kan leiden tot schendingen van de GDPR.

Opslag in internationale datacenters
Gegevens worden opgeslagen in landen zonder adequate beveiliging of privacywetgeving, wat risico's verhoogt.

Juridische en financiële schade
De opeenstapeling van fouten resulteert in boetes, datalekken en reputatieschade.



Hoe een private cloud infrastructuur helpt bij GDPR- en AI Act-compliance.

Het opzetten van een private cloud infrastructuur kan grote voordelen bieden voor organisaties die AI gebruiken en willen voldoen aan wet- en regelgeving van de EU:

- **Betere controle over gegevens:** in een private cloud heeft een organisatie volledige controle over de infrastructuur, waardoor men in staat is om nauwkeurig te bepalen waar en hoe gegevens worden opgeslagen, verwerkt en beveiligd.
- **Geografische locatie:** organisaties kunnen ervoor zorgen dat gegevens worden opgeslagen in een land of regio die voldoet aan de EU-eisen.
- **Toegangscontrole:** organisaties kunnen strengere toegangsbeperkingen instellen voor wie toegang heeft tot persoonsgegevens.
- **Gegevensminimalisatie:** organisaties hebben volledige controle over hoeveel en welke gegevens worden verzameld en verwerkt.
- **Dataopslag en -verwerking:** organisaties kunnen instellen welke specifieke gegevens worden verzameld, opgeslagen en geanalyseerd.
- **Versleuteling en beveiliging van gegevens:** een van de belangrijkste eisen van de EU is dat persoonsgegevens veilig moeten worden verwerkt. Met een private cloudoplossing kunnen organisaties sterke beveiligingsmaatregelen nemen
- **End-to-end encryptie:** organisaties kunnen ervoor zorgen dat alle data, zowel in rust als tijdens overdracht, versleuteld is.
- **Vaststellen van interne beveiligingsmaatregelen:** organisaties kunnen specifieke beveiligingsmaatregelen implementeren die zijn afgestemd op hun eigen behoeften.
- **Gegevensbeheer en -verwerking:** organisaties krijgen meer mogelijkheden voor het beheren van gegevensverwerkingsactiviteiten, zoals het verkrijgen van expliciete toestemming van gebruikers.
- **Geautomatiseerde processen:** de infrastructuur kan processen zoals data-anonimisering en pseudonimisering automatiseren.
- **Toestemmingsbeheer:** organisaties kunnen mechanismen implementeren om toestemming van gebruikers voor dataverzameling en verwerking te verkrijgen en bij te houden.
- **Automatisering van verzoeken:** de private cloud biedt de benodigde flexibiliteit en snelheid om verzoeken van betrokkenen snel te verwerken.

- **Gedetailleerde logs:** auditlogs die gedetailleerd vastleggen wie op welk moment toegang heeft gehad tot welke gegevens en wat men ermee gedaan heeft kunnen worden bijgehouden.
- **Transparantie in AI-modellen:** modellen kunnen ook worden geëvalueerd en geanalyseerd op vooroordelen, transparantie en de verwerking van gegevens.
- **Incidentbeheer:** organisaties krijgen tools voor real-time monitoring en incidentbeheer voor snel en effectief reageren.

Privacy by design en Privacy by default.

Een private cloud biedt de nodige controle en flexibiliteit voor organisaties om de principes van Privacy by design en Privacy by default te implementeren. Door vanaf het begin privacy maatregelen te integreren en standaardinstellingen te configureren kunnen zij ervoor zorgen dat ze voldoen aan EU-eisen.

Privacy by design betekent dat privacybescherming vanaf het begin wordt ingebouwd in een systeem of proces. In een private cloud kunnen organisaties de infrastructuur volledig zelf beheren en hebben ze de mogelijkheid om privacy in elke laag van de infrastructuur te integreren.

Privacy by default betekent dat de cloudconfiguratie zo wordt ingesteld dat de privacy van gebruikersdata wordt gewaarborgd, zelfs voordat de organisatie wijzigingen aanbrengt.

Zo implementeer je een GDPR-compliant AI-oplossing.

Voor de implementatie van een oplossing waarmee je voldoet aan de eisen van de EU zijn de volgende stappen noodzakelijk:

1

Stap 1: Voer een data-audit uit
Zorg dat je weet welke data jouw AI gebruikt en hoe deze wordt verwerkt.

2

Stap 2: Kies een private cloud voor AI
Gebruik een veilige private cloud infrastructuur om volledige controle over gegevens te behouden.

3

Stap 3: Integreer transparantie en toestemming
Zorg ervoor dat alle gegevensverwerking transparant is en dat de juiste toestemming van gebruikers is verkregen.

4

Stap 4: Monitor compliance
Gebruik tools en dashboards om AI-gebruik te monitoren en ervoor te zorgen dat je altijd aan de eisen voldoet.

Conclusie.

Samen bieden de GDPR en EU AI Act een robuust kader dat de bescherming van persoonsgegevens en de veiligheid en transparantie van AI-systemen in de Europese Unie waarborgt. Een private cloud infrastructuur is hierbij voor bedrijven essentieel. Het stelt hen in staat om met gemak de controle over hun data te behouden, geavanceerde beveiligingsmaatregelen te implementeren en zo het vertrouwen te kunnen garanderen waar klanten om vragen.

Fuse AI –
De oplossing van Uniserver.

Uniserver introduceert Fuse AI, een oplossing waarmee bedrijven op een veilige, gemakkelijke en gecontroleerde manier Private AI kunnen inzetten zonder dat gevoelige data de organisatie verlaat.

Deze dienst speelt in op de groeiende behoefte aan privacy en dataveiligheid bij het gebruik van AI. Waar het grootste deel van de AI-oplossingen doorgaans in publieke cloudomgevingen draait, zorgt Private AI ervoor dat jouw data lokaal blijft in onze eigen soevereine cloudomgeving. Dit resulteert in een hogere mate van dataprivacy en controle.

Het betekent dat je jouw eigen 'ChatGPT'-interface kunt opzetten, inclusief het gebruik van je eigen datasets, zonder afhankelijk te zijn van publieke cloudproviders zoals Microsoft of Google. Zo is Private AI ideaal voor organisaties die maximale databeveiliging eisen en toch willen profiteren van AI-mogelijkheden.

Wil je meer te weten komen over Fuse Private AI?

Bekijk hier meer informatie en vraag een demo aan.

Over ons.

Uniserver, opgericht in 2000, is een vooraanstaande aanbieder van soevereine private cloud-oplossingen in Nederland. Wij maken de kracht van cloud toegankelijk voor alle sectoren – van zorg en finance tot overheid en retail. Onze private cloud-oplossingen zijn speciaal ontworpen om te voldoen aan de hoogste eisen, waarbij veiligheid en betrouwbaarheid voorop staan. Gehost in Nederlandse datacenters, waarborgen onze oplossingen volledige data-soevereiniteit.

Als onderdeel van de Atomic Group, werken we nauw samen met CloudNation en RevoData om naadloze integraties en superieure cloudoplossingen in private, publieke en hybride omgevingen te bieden. Onze aanpak is gericht op het vereenvoudigen van complexe cloud-uitdagingen, waardoor onze klanten kunnen focussen op wat echt belangrijk is: groei en innovatie. Uniserver staat voor geavanceerde technologie, operationele excellentie en onvoorwaardelijke klanttevredenheid.