NOREA Data Privacy Dag Update

Het belang van DPIA's voor hoogrisico-AI-systemen die persoonsgegevens verwerken

De snelle ontwikkeling van kunstmatige intelligentie (AI) biedt geweldige kansen, maar brengt ook aanzienlijke uitdagingen met zich mee, vooral wanneer hoogrisico-AI-systemen persoonsgegevens verwerken. Een Data Protection Impact Assessment (DPIA) is essentieel om potentiële risico's voor de rechten en vrijheden van individuen te identificeren, te beoordelen en te beperken bij het gebruik van AI-systemen in het algemeen, en hoogrisico-AI-systemen in het bijzonder.

Wat zijn hoogrisico-AI-systemen?

Hoogrisico-AI-systemen, zoals gedefinieerd door regelgeving zoals de EU AI_Act, zijn systemen die aanzienlijke risico's opleveren voor de gezondheid, veiligheid of fundamentele rechten van individuen. Bij het verwerken van persoonsgegevens worden deze risico's op het gebied van privacy versterkt. DPIA's zijn in deze gevallen bijzonder belangrijk omdat ze organisaties helpen bij het identificeren en aanpakken van mogelijke vooroordelen, discriminerende resultaten en andere negatieve effecten op individuen.

Waarom DPIA's essentieel zijn voor hoogrisico-AI-systemen

DPIA's zijn cruciaal voor hoogrisico-AI-systemen die persoonsgegevens verwerken vanwege hun rol bij het identificeren en beperken van potentiële risico’s met betrekking tot de privacy van betrokkenen wiens persoonsgegevens worden verwerkt.

Artikel 26(9) van de AI Act stelt dat de AI systeem gebruiker (deployer) van hoogrisico-AI-systemen de door AI systeemontwikkelaar/leverancier (provider) verstrekte informatie (met betrekking tot het doel, de prestaties en de risico's van het AI-systeem) moeten gebruiken om te voldoen aan hun DPIA-verplichtingen onder Artikel 35 van de AVG.

De NOREA DPIA biedt een raamwerk dat deployers kan helpen bij het nakomen van deze verplichting. Dit raamwerk, ontwikkeld door de Nederlandse Orde van IT-auditors (NOREA), biedt praktische richtlijnen en tools voor het uitvoeren van DPIA's. Het sluit aan bij internationale normen en voorschriften zoals de AVG en de EU AI-Act, en biedt een gestructureerde aanpak voor het beoordelen en beperken van gegevensbeschermingsrisico's.

Hoe de huidige NOREA DPIA helpt bij het voldoen aan Artikel 26(9) van de AI Act

Informatie van de provider: De NOREA DPIA benadrukt het belang van het begrijpen van de context van het AI-systeem, inclusief het doel, de gegevensbronnen en de verwerkingsmethoden. Dit komt overeen met de eis van Artikel 26(9) om de informatie van de provider over het AI-systeem te gebruiken.

Risicobeoordeling: De NOREA DPIA omvat een risicobeoordeling, die essentieel is voor het identificeren en beoordelen van de specifieke risico's voor de privacy rechten en vrijheden van individuen die door het AI-systeem worden veroorzaakt, zoals vereist door Artikel 26(9) en Artikel 35 van de AVG.

Risicobeperking: De NOREA DPIA richt zich op het ontwikkelen en implementeren van passende risicobeperkende maatregelen. Dit is in lijn met de eis van Artikel 26(9) om passende maatregelen te nemen om de geïdentificeerde risico's te beperken.

Documentatie: De NOREA DPIA vereist documentatie van het DPIA-proces en de bevindingen. Dit helpt deployers om aan de documentatie-eis van Artikel 26(9) te voldoen.

Toekomstige aanvullingen op de NOREA DPIA

In 2025 wordt een nieuwe versie van de NOREA DPIA uitgebracht. De belangrijkste aanpassingen zullen plaatsvinden op de volgende onderwerpen:

Beschrijving gegevensverwerking (deel I). Herijking van de huidige vragen met betrekking tot de contextanalyse en de verschillende fasen van de informatie levenscyclus; kan het worden vereenvoudigd/kunnen er vragen weg en dienen er mogelijk vragen te worden toegevoegd naar aanleiding van ontwikkelingen vanuit de EDPB, wet en regelgeving en jurisprudentie zoals de EU AI-Act. Een voorbeeld hiervan is monitoring: Op de daartoe geëigende plaatsen zal additionele nadruk worden gelegd op de *plan do check act cycle* en daarmee ook continue monitoring van het AI-systeem te borgen. Dit helpt *deployers* om de DPIA up-to-date te houden, zoals vereist door Artikel 26(9).

Risk assessment & treatment (deel III). Beoordeling of de beschrijving van risicobeoordeling op basis van de Bowtie-techniek vereenvoudigd kan worden en of bij het definiëren van de maatregelen om de privacy-risico's te mitigeren gebruik kan worden gemaakt van Privacy by Design-ontwerpprincipes.

Na het uitbrengen van de nieuwe versie van de NOREA DPIA zal ook gewerkt worden aan een Engelstalige versie.

Conclusie

Het NOREA DPIA-raamwerk helpt organisaties bij het navigeren door de complexiteit van AI-gegevensbescherming, het waarborgen van naleving, het beperken van risico's en het bevorderen van vertrouwen, terwijl het innovatie en het gunstige gebruik van AI voor alle belanghebbenden stimuleert. Het dient ook als een waardevolle randvoorwaarde voor het aanpakken van privacyaspecten binnen bredere Fundamental Rights Impact Assessments voor AI-systemen met een hoog risico. Door het raamwerk te onderhouden en bij te werken, zorgt NOREA ervoor dat het voortdurend is afgestemd op de vereisten en verplichtingen die voortvloeien uit nieuwe wetten, voorschriften en best practices.