Auteur: Arnoud Engelfriet is informaticus en IT-jurist. Hij verdiept zich graag in complexe uitdagingen op het snijvlak van ICT en recht. Arnoud staat aan het hoofd van de Academy waar hij diverse IT-gerelateerde cursussen voor juridische en zakelijke professionals heeft ontwikkeld. Arnoud nam het initiatief tot het creëren van de gecertificeerde CAICO®-cursus voor AI Compliance Officers. Hij blogt sinds 2007 elke werkdag over IT-recht en technologie en is bereikbaar via a.engelfriet@ictrecht.nl.

Risicobeheersing: de AI Act en de AVG

De AI Act doet iets aparts: deze reguleert AI niet in het algemeen, maar focust op de beheersing van risico's van deze innovatieve technologie. De wet kent daartoe diverse instrumenten, waarvan de conformiteitsbeoordeling (Conformity Assessment) de belangrijkste is. Deze lijkt op de Data Protection Impact Assessment (DPIA) die we al kennen uit de AVG, maar er zijn belangrijke verschillen. Hoe werkt de AI Act?

De AI Act kent drie risiconiveaus: verboden, hoogrisico en laagrisico. De meeste eisen gaan gelden voor AI-systemen die een hoog risico vormen voor de gezondheid, veiligheid, grondrechten of het milieu. Zo moet duidelijk zijn waar de data vandaan komt waarmee de AI is getraind, is menselijk toezicht vereist en moet de technische documentatie op orde zijn. Het afhandelen van verzekeringsclaims, bepaalde medische hulpmiddelen en algoritmes die sollicitanten beoordelen zijn voorbeelden van hoog risico-AI.

Bepalen of een AI hoogrisico of verboden is, is een kwestie van inschatten of de toepassing binnen een bepaalde lijst valt. Het is dus geen open norm waarbij je voors en tegens tegen elkaar afweegt, zoals bij de vraag of je een DPIA moet uitvoeren onder de AVG. Het omgekeerde is wel waar: als een AI hoog risico is en persoonsgegevens verwerkt, dan is een DPIA verplicht.

Doel van conformiteitsbeoordelingen

Het doel van conformiteitsbeoordelingen (conformity assessments of CA's) is het toetsen aan normen en beheersen van risico's. In de AI Act is het doel specifiek het toetsen aan specifieke wettelijke vereisten voordat deze op de Europese markt worden gebracht. De verantwoordelijkheid voor het uitvoeren van deze beoordelingen ligt primair bij de aanbieders van deze systemen, maar kan ook betrekking hebben op fabrikanten, distributeurs of importeurs. Dit proces benadrukt de noodzaak van transparantie en accountability in de ontwikkeling en implementatie van AI-systemen.
De opstellers van de AI Act zetten hierbij zwaar in op Europese normen waarmee het assessment kan worden uitgevoerd. Voldoet men aan deze normen, dan wordt de conformiteit verondersteld te bestaan. Zijn er geen relevante normen of standaarden te vinden, dan gelden de normen uit Annex VII van de AI Act.

Verantwoordelijke partij

Een CA moet worden uitgevoerd voordat een AI-systeem op de EU-markt beschikbaar komt. Dat kan simpelweg zijn doordat producten met de AI erin worden verkocht, maar ook door het aanbieden van een online dienst of app met daarin verweven de AI. Ook wanneer een bedrijf voor eigen toepassing een AI ontwikkelt, moet de CA worden uitgevoerd voordat deze in gebruik wordt genomen.
Een CA is niet een eenmalige exercitie. Als het AI-systeem aanzienlijk wordt gewijzigd, moet de CA opnieuw worden uitgevoerd. Het enkele feit dat het AI-systeem bijleert en daarmee nieuw gedrag vertoont, is echter niet genoeg om een nieuwe CA te hoeven doen. Wel moet in de CA natuurlijk zijn opgenomen dat het systeem kan bijleren.

De CA wordt primair uitgevoerd door de provider van het AI-systeem. Als deze dat nalaat, dan kunnen de importeur of deployer van het systeem deze taak op zich nemen om er zo voor te zorgen dat het AI-systeem (of product met de AI erin) alsnog de Europese markt op kan. Een partij is de provider als deze de AI op de markt brengt met een eigen merknaam. Dit hoeft dus niet de feitelijke ontwikkelaar te zijn.

Wijze van uitvoering

Er zijn twee manieren waarop een CA kan worden uitgevoerd: intern of door een derde partij. In het interne CA-proces is het de provider zelf (of de distributeur/importeur/deployer) die de CA uitvoert. De CA door een derde partij wordt uitgevoerd door een externe zogeheten 'notified body'. Deze 'aangemelde instanties' zijn conformiteitsbeoordelingsinstanties die aan specifieke vereisten voldoen en zijn aangewezen door de nationale notifying authorities.

Uitgangspunt is dat een provider werkt met een interne CA. De provider zal immers beter uitgerust zijn en de nodige expertise hebben om de naleving van AI-systemen te beoordelen. Alleen bij de inzet van realtime en post remote biometrische identificatie van personen is dit niet mogelijk. En wanneer het product op de wettenlijst van Bijlage II staat (dus hoog risico vanwege veiligheidscomponent) dan moet uit de toepasselijke wet volgen welke keuze van intern of extern wordt gemaakt.

Bij een interne CA moet de provider:

1. Verifiëren dat het vastgestelde kwaliteitsmanagementsysteem in overeenstemming is met de vereisten;
2. De informatie in de technische documentatie onderzoeken om te beoordelen of aan de vereisten is voldaan;
3. Verifiëren dat het ontwerp- en ontwikkelingsproces van het AI-systeem en de post-markt monitoring consistent is met de technische documentatie.

Na het uitvoeren van een interne CA stelt de verantwoordelijke entiteit een schriftelijke EU-conformiteitsverklaring op voor het AI-systeem. Bijlage V van de AI Act somt de informatie op die moet worden opgenomen in de EU-conformiteitsverklaring. Deze verklaring moet actueel worden gehouden tot tien jaar

De AVG kent geen sjabloon of voorbeeld van hoe een DPIA eruit moet zien

nadat het systeem op de markt is gebracht of in gebruik is genomen. De provider moet ook een zichtbare, leesbare en onuitwisbare CE-markering van conformiteit aanbrengen. En als laatste moet de provider een EU-verklaringsformulier opstellen met daarin onder meer een beschrijving van de uitgevoerde procedure. In het geval van een CA door een derde partij beoordeelt de notified body het kwaliteitsmanagementsysteem en de technische documentatie. De provider doet hiertoe een verzoek en moet de benodigde informatie aanleveren. Bijlage VII somt de informatie op die moet worden opgenomen in de aanvraag aan de aangemelde instantie. Zowel het kwaliteitsmanagementsysteem als de technische documentatie moeten in de aanvraag staan.
Als de aangemelde instantie vaststelt dat het hoog risico-AI-systeem in overeenstemming is met de vereisten, zal het een EU-certificaat van technische documentatiebeoordeling afgeven dat een beperkte geldigheid heeft. Net zoals bij de interne CA, moet de provider onder het CA-proces door een derde partij de EU-conformiteitsverklaring opstellen en de CE-markering van conformiteit aanbrengen. Om het proces af te ronden, moet de aanbieder een EU-verklaringsformulier opstellen met daarin onder meer een beschrijving van de uitgevoerde conformiteitsbeoordelingsprocedure.

In het geval de aangemelde instantie beoordeelt dat het hoog risico-AI-systeem niet in overeenstemming is met de vereisten voor hoog risico-AI-systemen, moet dit gedetailleerd worden gecommuniceerd en uitgelegd aan de aanbieder of andere verantwoordelijke entiteit. Artikel 45 geeft de provider het recht om beroep aan te tekenen tegen de beslissing van de aangemelde instantie. Als het oordeel overeind blijft, kan de provider worden bevolen het systeem aan te passen, terug te trekken of van de markt te halen.

Let op: de CA is geen eenmalige oefening. Providers moeten een post-markt monitoringssysteem opzetten en documenteren, dat tot doel heeft de voortdurende naleving van AI-systemen met de AIA-vereisten voor hoog risico-AI-systemen te evalueren. Het post-markt monitoringsplan kan deel uitmaken van de technische documentatie of het productplan. Daarnaast moet in het geval van een externe CA partij de notified body periodieke audits uitvoeren om ervoor te zorgen dat de provider het kwaliteitsmanagementsysteem handhaaft en toepast.

Data Protection Impact Assessments

Het instrument van de Data Protection Impact Assessment of DPIA (in het Nederlands: gegevensbeschermingseffectbeoordeling) is in de AVG opgenomen om bepaalde risico's en gevolgen van verwerken van persoonsgegevens te kunnen beheersen. Vanwege deze insteek lijken er overeenkomsten te zijn met een CA. Toch zijn er belangrijke verschillen.

Doel van de DPIA

De DPIA is een wettelijke verplichting onder de AVG die vereist dat de entiteit verantwoordelijk voor een verwerking van persoonsgegevens (de 'controller') een beoordeling uitvoert van de impact van de beoogde verwerking op de

bescherming van persoonsgegevens, in het bijzonder wanneer de betreffende verwerking waarschijnlijk een hoog risico vormt voor de rechten en vrijheden van individuen, voordat de verwerking plaatsvindt.

Doel van de DPIA is het beoordelen van noodzaak en evenredigheid van de verwerkingen en de risico's die daarmee samengaan, en het formuleren van maatregelen om deze te mitigeren. Deze dient voorafgaand aan het starten van de verwerking te worden uitgevoerd (net zoals de CA), en kan leiden tot de plicht om toestemming te vragen aan de toezichthouder voordat de verwerking wordt ingezet. Is die plicht er niet, en meent de controller dat de risico's adequaat bestreden zijn, dan mag men de keuze maken de markt op te gaan.

Dit is iets anders dan bij de CA: daar mag het gebruik van het AI-systeem pas beginnen nadat het systeem conform is gemaakt en het CE-logo aangebracht is. Er is geen optie om bijvoorbeeld een ontheffing te vragen als de conformiteitsbeoordeling niet slaagt.
De AVG kent geen sjabloon of voorbeeld van hoe een DPIA eruit moet zien. Ook zegt de AVG niet welke maatregelen zouden passen bij welke risico's. Er zijn ook geen normen waarmee men compliance aan de AVG kan vaststellen. Dit maakt een DPIA meer open-ended dan een CA.

Verantwoordelijke partij

Onder de AVG is de datacontroller of verwerkingsverantwoordelijke de partij die de doelen en middelen van de verwerking van persoonsgegevens bepaalt. De datacontroller is dan ook verantwoordelijk voor alle compliance aspecten van de AVG, en dus ook voor het beoordelen of een DPIA moet worden uitgevoerd en voor het feitelijk uitvoeren daarvan. Uiteraard mag de controller ook anderen inhuren, of informatie gebruiken die een verwerker hem aanlevert.
In ICT in het algemeen, en bij AI in het bijzonder, heeft die verwerker vaak een zeer sturende en prominente rol. Wie bijvoorbeeld een SaaS-dienst afneemt en daarmee persoonsgegevens verwerkt, is volgens de AVG de 'controller' ook al kan hij feitelijk niets veranderen aan hoe de dienst werkt en is de inspraak vooral theoretisch. Als die dienst AI gebruikt, dan is de aanbieder van de SaaS-dienst de 'provider' daarvan en de afnemer de 'deployer'. Daarmee ligt dus de plicht tot een DPIA bij de afnemer, en de plicht tot een CA bij de leverancier.

Het kan dus zijn dat relevante delen van de CA uitgevoerd door de provider van het AI-systeem (zoals die gerelateerd aan de naleving van de gegevenskwaliteit en cybersecurity vereisten) vervolgens gebruikt worden om de afnemer te informeren, waarna die deze gegevens overneemt in de DPIA.
Net als bij de CA is een DPIA geen eenmalige exercitie. In de Guidelines over DPIA's geeft de EDPB duidelijk aan dat dit een continu proces van bijwerken en bijsturen is.

Wijze van uitvoering

De AVG bepaalt geen formeel proces voor het uitvoeren van een DPIA. De controller is de verantwoordelijke partij. Deze kan ervoor kiezen een derde het werk te laten uitvoeren, en mag zoals gezegd afgaan op informatie van de verwerker, maar blijft eindverantwoordelijk voor de juistheid en actualiteit van de DPIA. Is er een functionaris gegevensbescherming, dan moet deze worden geraadpleegd. Ook moet de controller waar relevant de input van betrokken personen verkrijgen. De CA procedure kent dit laatste aspect niet, hoewel het ook niet verboden is om bij het proces input van personen van buitenaf te verkrijgen.
Zowel de DPIA als de CA focussen op risico's van buitenaf. De scope is wel iets anders: bij een DPIA gaat het om risico's die verband houden met gebruik van persoonsgegevens, terwijl bij een CA het gaat om alle risico's die het AI-systeem kan veroorzaken of verhogen. Een risico op het vernielen van vloerbedekking door een robotstofzuiger zal bijvoorbeeld wél in een CA aan de orde moeten komen, maar in een DPIA niet relevant zijn.

Bij een CA wordt in principe uitgegaan van normen waartegen men het assessment maakt. Voor DPIA's zijn dergelijke normen er niet. Diverse handreikingen en modellen voor DPIA's verwijzen naar ISO-norm 31000, de internationale norm voor risicomanagement. Het is echter geen gegeven dat dit de juiste norm is voor een specifieke organisatie.

De inhoud van een DPIA hoeft niet openbaar gemaakt te worden. Vaak zien organisaties deze ook als bedrijfsgeheim. Ook een CA hoeft niet gepubliceerd te worden. Bij beiden geldt wel dat de toezichthouder inzage mag eisen in deze documenten. Onder artikel 51 moet de provider van een hoog risico AI wel een samenvatting van de DPIA aanleveren voor publicatie in de openbare database van deze AI's.

Samenloop van CA en DPIA

Organisaties die AI op de markt brengen of inzetten, kunnen zowel met een CA als met een DPIA te maken krijgen. Een DPIA focust op beheersen van risico's rondom persoonsgegevens, terwijl een CA een proces biedt voor het mitigeren van risico's rondom AI. Hoewel er dus zeker overeenstemmingen zijn, is het zeker geen gegeven dat het uitvoeren van een DPIA ertoe leidt dat de CA overbodig is – of andersom. Let dus goed op de vereisten van beiden.