Data-ethiek en privacy: moeten, kunnen, willen?

Ethische vraagstukken bij het gebruik van technologie zoals kunstmatige intelligentie (in het Engels: *artificial intelligence,* ofwel AI) spelen een grote rol in onze samenleving. En niet zonder reden: nu we steeds vaker te maken hebben met publieke schandalen die samenhangen met het verkeerd gebruik van data, is de roep om een ethisch en privacyverantwoord beleid steeds groter. Daarbij staat het vertrouwen van klanten, medewerkers en burgers in publieke en private organisaties op het spel. De kritieke vraag voor organisaties is dan ook: hoe halen we het meest uit wat de data en technologie ons bieden terwijl we tegelijkertijd de ethische aspecten en privacy-aspecten bewaken?

Dit artikel gaat nader in op wat data-ethiek is en wat de raakvlakken met privacy zijn, bespreekt nieuwe juridische ontwikkelingen en geeft praktische tips over hoe een start te maken het inrichten en versterken van data-ethiek in organisaties.

Marijn Bakker LL.M., CIPM, CIPP/E,
is Data Privacy Manager bij KPMG Cyber & Privacy.

Sterre Stolk LL.M.
was privacy consultant bij KPMG Nederland.

INLEIDING

Op 25 mei 2023 bestaat de Europese privacywet, de Algemene verordening gegevensbescherming (AVG), vijf jaar. Bij veel organisaties is privacybescherming niet meer weg te denken uit de bedrijfsvoering. Reden voor een feestje in mei 2023? Niet helemaal.

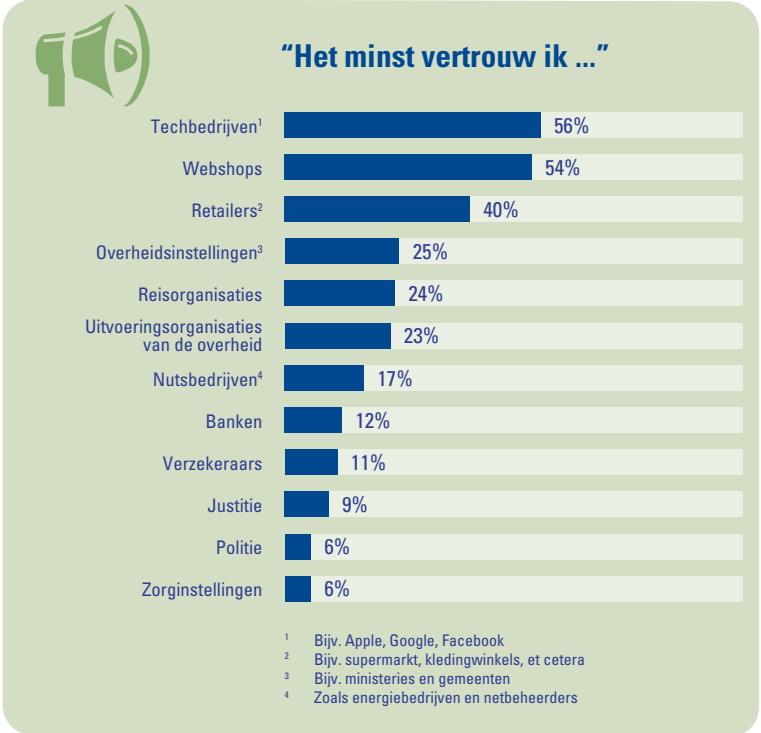
Het vertrouwen van Nederlanders dat bedrijven en overheidsorganisaties goed met hun privacy omgaan blijft laag. Dit constateerde KPMG in 2021 in een privacyonderzoek onder Nederlanders getiteld 'Meer zorgen over privacy' ([KPMG21]). Zo bleek uit het onderzoek dat een kwart van de Nederlanders een behoorlijk wantrouwen jegens de overheid koestert en hun vertrouwen in technologiebedrijven nog geringer is. Dit uit zich in een groeiende bezorgdheid over de eigen privacy.

Waar het vertrouwen in overheidsinstanties en bedrijven daalt, neemt de belangstelling voor privacy toe. Een overgrote meerderheid van de Nederlanders (86 procent) vindt het goed dat er veel aandacht is voor privacy ([KPMG21]). Dat is fors meer dan begin 2018, toen uit het KPMG-onderzoek 'Een beetje privacy graag' bleek dat 69 procent privacy een belangrijk thema vond ([KPMG18]; zie ook [ICTM18]). Daarnaast wordt deze belangstelling bevestigd door het feit dat Nederland binnen de Europese Unie een van de koplopers is wat betreft het melden van datalekken ([DLAP21]). Een verklaring voor deze toenemende aandacht voor privacy ligt in de verdere ontwikkelingen in de digitale transformatie die de samenleving doormaakt en waarbij de vraag steeds nadrukkelijker naar voren komt: hoe verantwoord of ethisch zijn alle technische ontwikkelingen die elkaar in relatief korte tijd opvolgen?

De Autoriteit Persoonsgegevens (AP) concludeerde in haar jaarverslag over het jaar 2021 dat de samenleving op het punt is gekomen dat digitalisering niet langer zonder ethische waardenafweging kan ([AP22b]). In hun privéleven, als consument en als burger, worden mensen continu geconfronteerd met nieuwe technologieën, al zullen ze dat niet altijd doorhebben. Technologieën zoals algoritmes hebben een structurele plek in ons dagelijks leven ingenomen. Of het nu gaat om het doen van een aankoop in een webwinkel en achteraf betalen, het afsluiten van een lening bij een bank of het aanvragen van een subsidie bij de overheid, de kans is groot dat de aanvraag wordt beoordeeld met gebruik van technologieën.

Nieuwe technologieën brengen geweldige mogelijkheden met zich mee voor het ontwikkelen van nieuwe producten en diensten, het zorgen voor een betere klantervaring en het slimmer inrichten van werk. Maar om uiteindelijk succesvol gebruik te kunnen blijven maken van technologieën, dienen organisaties die verantwoord te gebrui-

Figuur 1. Het vertrouwen in de overheid is niet erg groot, maar het vertrouwen in grote technologiebedrijven blijkt nog veel geringer ([KPMG21]).



ken. Hierbij spelen data-ethiek en privacy een essentiële rol. De AVG biedt handvatten voor het ethisch gebruik van persoonsgegevens, maar data-ethiek is breder dan enkel het verzamelen, gebruiken, bewaren en verwijderen van persoonsgegevens.

WAT IS DATA-ETHIEK?

Ethiek gaat over goed en fout. Over wat de maatschappij, burgers of consumenten eerlijk, rechtvaardig en aanvaardbaar vinden ([Meel]). Vanuit het privacyperspectief bekeken, gaat data-ethiek niet zozeer over de vraag of een organisatie persoonsgegevens mag verwerken en of de verwerking voldoet aan de vereisten van de AVG, maar over een vraagstuk dat fundamenteler van aard is. Het gaat namelijk over de volgende afweging: ook al *moeten* of *mogen* organisaties iets (bijvoorbeeld vanuit juridisch perspectief), en ook al *kunnen* zij iets (bijvoorbeeld vanuit technisch perspectief), organisaties moeten zichzelf continu de vraag stellen of ze het vanuit ethisch perspectief ook *willen*. Ofwel: het mag wel, maar deugt het ook?

Data-ethiek vereist een andere manier van denken binnen een organisatie waarbij de focus ligt op wat de impact van een dataverwerking op de mens en de maatschappij is. Data-ethiek draait om de vraag: is wat we willen, mogen of moeten doen vanuit ethisch perspectief ook het juiste om te doen? Een privacyprofessional kan raakvlakken zien met het uitvoeren van een Data Protection Impact Assessment (DPIA) waarbij de privacyrisico's van een verwerking voor betrokkenen in kaart worden gebracht. Data-ethiek is echter veel breder dan privacy. Data-ethiek gaat over non-discriminatie, het voorkomen van bias en het transparant en verantwoordelijk handelen jegens mensen die de gevolgen ondervinden van het gebruik van technologie. Het voorbeeld in het kader hiernaast illustreert dit ([Ober19]).

Een ziekenhuis in de Verenigde Staten maakte gebruikt van een commercieel algoritme om te bepalen welke groep patiënten mogelijk meer zorg nodig zou hebben dan gemiddeld. In de Verenigde Staten wordt veel gebruikgemaakt van algoritmes door onder andere ziekenhuizen, overheidsinstanties en andere zorgaanbieders. Naar schatting worden jaarlijks ongeveer 200 miljoen mensen beoordeeld met behulp van dergelijke algoritmes.

In deze casus rangschikte een algoritme patiënten op basis van de mate waarin zij gebruikmaakten van medische zorg. Patiënten in het 97e percentiel en hoger werden door het algoritme gemarkeerd als 'hoog risico' en werden automatisch ingeschreven voor een gezondheidsprogramma. Het willen verbeteren van de gezondheid van hoog-risicopatiënten is een nobel doel, maar achteraf bleek dat er een bias op basis van ras aanwezig was in het algoritme. Volgens het algoritme zijn patiënten van kleur gezonder dan witte patiënten, maar dit bleek een verkeerde conclusie te zijn.

De reden voor deze bias was te herleiden naar de invoerdata. Mensen van kleur maken minder gebruik van zorg dan witte mensen en geven gemiddeld 1.800 dollar minder uit per jaar aan zorg dan die groep. Het algoritme heeft hieruit afgeleid dat zwarte mensen dan gezonder moesten zijn, aangezien zij minder gebruikmaken van gezondheidszorg. Dit bleek echter een verkeerde conclusie te zijn. Daarnaast bestond de dataset waar het algoritme op gebaseerd was, uit 44.000 witte patiënten en slechts 6.000 patiënten van kleur. Door deze beperkte invoerdata nam het algoritme verkeerde besluiten en had het een negatieve impact op de toegang tot de gezondheidszorg voor een bepaalde groep mensen.

JURIDISCHE ONTWIKKELINGEN OP HET GEBIED VAN DATA-ETHIEK: DE AI ACT

Wanneer het in het maatschappelijke debat gaat over data-ethiek, gaat het met regelmaat over de betrouwbaarheid en toenemende inzet van data en algoritmes bij private en publieke organisaties en hoe er op een gecontroleerde en ethische manier gebruik kan worden gemaakt van algoritmes. De Europese Commissie heeft wereldwijd het voortouw genomen om het gebruik van kunstmatige intelligentie, in het Engels *artificial intelligence* (AI), te reguleren. Dit heeft geresulteerd in het wetsvoorstel genaamd de Artificial Intelligence Act, oftewel de AI Act.

De AI Act heeft tot doel een kader voor betrouwbare AI tot stand te brengen. Volgens het wetsvoorstel moeten AI-systemen juridisch, ethisch en technisch robuust zijn en moeten ze democratische waarden, mensenrechten en de rechtsstaat respecteren. Het feit dat de AI Act ingaat op juridische en technische regulering van AI, is niet verrassend. Wat echter nieuw is, is de sterke nadruk op data-ethiek. Het streven is dat er dit jaar (2023) een definitief akkoord wordt bereikt over de AI Act, al is er geen concrete deadline. Wanneer een akkoord wordt bereikt, zal er een periode van circa twee jaar volgen voordat de AI Act daadwerkelijk in werking zal treden.

Het wetsvoorstel voor de AI Act introduceert nieuwe verplichtingen voor bedrijven en overheden, alsmede een toezichthoudende autoriteit en een boetesysteem. Deze worden in de onderstaande paragrafen nader toegelicht. Hierbij is het van belang te benadrukken dat er nog geen definitief akkoord is bereikt over de exacte inhoud van de AI Act. Met andere woorden, de juridische ontwikkelingen (en voorgestelde aanpassingen op de AI Act[1]) volgen elkaar snel op. Zo kijkt men op dit moment naar aanpassingen in de AI Act om de ontwikkelingen rond ChatGPT en soortgelijke generatieve AI-modellen het hoofd te bieden. Oftewel, de juridische en technische ontwikkelingen die impact kunnen hebben op de AI Act, zijn het waard om in de gaten te houden.

Conformiteitsbeoordeling voor AI-systemen met een hoog risico

Het wetsvoorstel voor de AI Act introduceert het uitvoeren van een zogenoemde conformiteitsbeoordeling door een externe instantie. Met andere woorden, wanneer een AI-systeem een hoog risico zou kunnen vormen voor de gezondheid, veiligheid of grondrechten van mensen, moeten de aanbieders ervan een beoordeling laten uitvoeren door een onafhankelijke derde partij om de risico's in kaart te brengen. De conformiteitsbeoordeling heeft als doel de naleving op de AI Act te waarborgen. Voor AI-systemen met een beperkt of minimaal risico gelden minder zware eisen. Daar is bijvoorbeeld een self-assessment of transparantieverplichting voldoende.

In het wetvoorstel voor de AI Act staat op dit moment opgenomen dat de Europese Commissie het orgaan is dat bepaalt wat een hoog risicosysteem is en wanneer er een verplichte conformiteitsbeoordeling moet worden uitgevoerd. AI-systemen die mogelijk zullen kwalificeren als hoog risico, zijn onder andere systemen voor migratie en asiel, kritieke infrastructuur, wetshandhaving en productveiligheid. Daarnaast wordt op dit moment gekeken of generatieve AI-modellen zoals ChatGPT ook als hoog risico dienen te gelden.

Op basis van het wetsvoorstel is er ook de mogelijkheid dat een AI-systeem classificeert als een hoog-risicosysteem, maar dat een conformiteitsbeoordeling niet vereist is. In dergelijke gevallen volstaat het om een self-assessment uit te voeren. Op dit moment staat in het wetsvoorstel dat de Europese Commissie zal bepalen voor welke (hoog-risico-)AI-systemen een self-assessment dient te worden uitgevoerd.

AI-systemen die een hoog risico vormen, moeten volgens de AI Act aan strenge eisen voldoen voordat deze op de markt mogen worden gebracht. Maatregelen die volgens het wetsvoorstel geïmplementeerd dienen te worden, zijn onder andere het inrichten van een risicomanagementproces dat specifiek toeziet op de AI-toepassing, het stellen van hoge datakwaliteitseisen om discriminatie te voorkomen, het bijhouden van logboeken, het opstellen van verantwoordingsdocumentatie, het waarborgen van de transparantie, het inrichten van een systeem waarin mensen toezicht houden op de AI-toepassingen, en het waarborgen van beveiligings- en nauwkeurigheidsstandaarden.

AI-database voor hoog-risicosystemen

Een ander nieuw aspect van de AI Act ziet op het opzetten van een AI-database waarin hoog-risico-AI-systemen geregistreerd dienen te worden. In het wetsvoorstel staat op dit moment dat de database zal worden beheerd door de Europese Commissie en als doel heeft de transparantie te vergroten en het houden van toezicht door de toezichthouders te vergemakkelijken.

Introductie van nationale AI-toezichthouder

In het wetsvoorstel van de AI Act wordt op dit moment gesproken over een verplichting voor elke lidstaat tot het vormen of aanwijzen van een autoriteit die toeziet op de naleving van de AI Act. Deze nationale toezichthoudende autoriteit neemt deel in de European AI Board (EAIB), waar de Europese Commissie de voorzitter van zal zijn en waar ook de European Data Protection Supervisor (EDPS) aan zal deelnemen. Recent is de Autoriteit Persoonsgegevens aangewezen als algoritmetoezichthouder in Nederland. Met deze benoeming geeft Nederland alvast invulling aan de toekomstige verplichting uit de AI Act.

Boetes voor niet voldoen aan de AI Act

Net als de AVG zal de AI Act een boetesysteem bevatten. De zwaarste boete die volgens het wetsvoorstel kan worden opgelegd, is een boete van maximaal 30 miljoen euro of 6 procent van de wereldwijde jaaromzet, afhankelijk van wat het hoogste is. Dit ligt 2 procent hoger dan de hoogste boetecategorie van de AVG. Afgezien van de morele verplichting voor bedrijven om data-ethiek en privacy serieus te nemen, betekent dit dat het raadzaam is om AI-systemen in lijn met de aankomende AI Act in te richten om hoge boetes te voorkomen.

1 Er wordt op dit moment in Europa nog onderhandeld over de definitieve inhoud van de AI Act. Dit betekent dat dit artikel een inkijk geeft in de ontwikkelingen rondom de AI Act, maar geen zekerheid kan bieden over de definitieve inhoud van de AI Act.

HOE DATA-ETHIEK IN DE PRAKTIJK TE BRENGEN?

Dat de AI Act op termijn haar intrede zal maken is duidelijk. Desalniettemin is het belangrijk te realiseren dat wetgeving enkel een basis vormt en dat ethisch handelen meer vergt dan het voldoen aan nieuwe wetgeving. Wat kunnen organisaties vandaag doen om de ethische omgang met data te bevorderen en het bewustzijn in de organisatie te verhogen?

Neem contact op met de Privacy Officer

De zorgen die bestaan over AI-systemen gaan in veel gevallen over het gebruik van persoonsgegevens. Ondanks dat privacy en data-ethiek twee verschillende onderwerpen zijn, overlappen ze ook. Dit betekent dat wanneer een organisatie een Privacy Officer heeft aangesteld, deze naar alle waarschijnlijkheid al bezig is met ethische vraagstukken rondom het gebruik van persoonsgegevens.

De AVG kent namelijk de verplichting een DPIA uit te voeren op verwerkingen van persoonsgegevens die kunnen resulteren in een hoog privacyrisico. De verplichting tot het uitvoeren van een DPIA zal in veel gevallen ook gelden voor AI-systemen die persoonsgegevens verwerken. Ondanks dat in de AI Act de kwaliteit van AI-systemen centraal staat en in de AVG het gebruik van persoonsgegevens, komen de twee wetten samen wanneer in AI-systemen persoonsgegevens worden gebruikt. Een Privacy Officer kan dus een goed startpunt zijn om de organisatie voor te bereiden op de ophanden zijnde AI-wetgeving. De Privacy Officer kan namelijk helpen inventariseren welke systemen in de organisatie gebruikmaken van AI en of deze systemen mogelijk een hoog risico met zich meebrengen.

Stel een ethisch kader op

De eerste stap om data-ethiek in een organisatie te borgen is om vast te stellen wat ethisch omgaan met data specifiek inhoudt voor de organisatie. Dit kan door waarden en principes te formuleren, bijvoorbeeld in de vorm van een ethisch kader of ethisch kompas. Het is belangrijk dat de ethische principes goed aansluiten bij de cultuur en kernwaarden van de organisatie en herkenbaar zijn voor medewerkers uit alle lagen van de organisatie ([Meel]).

Organiseer onafhankelijk toezicht

Data-ethiek is een abstract onderwerp, maar behoeft wel een heel concrete invulling. De meeste organisaties zijn (nog) niet ingericht op het omgaan met nieuwe ethische dilemma's die ontstaan als nieuwe technologieën zoals algoritmes worden ingezet en er bestaat vaak geen

> Ethiek gaat over goed en fout. Over wat de maatschappij, burgers of consumenten eerlijk, rechtvaardig en aanvaardbaar vinden

Volgens het IAMA kan het besluitvormingstraject rondom algoritmen worden ingedeeld in drie hoofdfasen:

- Fase 1: voorbereiding. In deze fase wordt bepaald waarom een algoritme zal worden ingezet en wat daarvan de effecten zullen zijn.
- Fase 2: input en throughput. In deze fase gaat het om het 'wat' van de ontwikkeling van een algoritmisch systeem. In deze fase wordt bepaald hoe het algoritme eruit moet zien en van welke data gebruik wordt gemaakt om het algoritme te voeden. Fase 2 bestaat uit twee subfasen:
  - Fase 2a: data, of input. Het gaat hier om vragen waarbij steeds de inzet van bepaalde data en databronnen centraal staat.
  - Fase 2b: algoritme, of throughput. Het gaat hier om vragen omtrent het in te zetten algoritme en de werking en transparantie daarvan.
- Fase 3: output, implementatie en toezicht. In deze fase gaat het om het 'hoe' van het inzetten van het algoritme, dus om de vraag welke output het algoritme genereert, hoe dat een rol kan spelen in beleid of besluitvorming en hoe daarop toezicht kan worden gehouden.

Bron: [MBZK21]

controle op de integratie van ethische principes in de bedrijfsvoering. Een krachtig middel bij zowel het opstellen van ethische principes als bij het gat dichten tussen principes en praktijk, is het inrichten van effectief en onafhankelijk toezicht. Dit kan door een onafhankelijke commissie, interne auditteams of een externe partij ([Meel]).

Voer een Impact Assessment Mensenrechten en Algoritmes uit

Wanneer een organisatie werkt met algoritmes, is het verstandig niet te wachten op de invoering van de AI Act en al een start te maken met het inventariseren van risico's tijdens het gebruik van algoritmes. Dit kan door een Impact Assessment Mensenrechten en Algoritmes (IAMA) uit te voeren. Het IAMA is ontwikkeld door de Utrecht Data School en helpt om zorgvuldige beslissingen te nemen over de inzet van algoritmes. Het IAMA is verplicht voor overheidsorganen, maar kan ook andere organisaties helpen een beter begrip te krijgen van de afwegingen en risico's die een rol spelen bij de besluitvorming rondom de inzet van algoritmes. Ook is het een manier om alvast te 'oefenen' met de ophanden zijnde assessments die de AI Act naar alle waarschijnlijkheid zal introduceren.

CONCLUSIE

Er is op dit moment nog geen sprake van een uitgekristalliseerd geheel van normen, wetten en jurisprudentie op het gebied van data-ethiek. Voorbeelden uit de dagelijkse praktijk laten zien dat dit wel hoog nodig is. Maar ook wanneer de AI Act eenmaal van kracht is, vraagt ethisch omgaan met data om meer dan het volgen van de letter van de wet. Neem het voorbeeld van de AVG, de Europese dataprivacywetgeving. De AVG geeft ons meer controle en beheersing over onze data, maar het ethische principe van privacy is een veel breder en abstracter thema dan alleen de bescherming van data. Een organisatie die de privacy van haar klanten als haar verantwoordelijkheid ziet, zal daarom verder moeten denken dan alleen het vermijden van een AVG-boete, of straks het vermijden van een AI Act-boete ([Meel]).

Literatuur

[AP22a] Autoriteit Persoonsgegevens (2022, 15 maart). *AP Inzet Artificial Intelligence Act.* Geraadpleegd van: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ap_inzet_ai_act.pdf

[AP22b] Autoriteit Persoonsgegevens (2021). *Jaarverslag 2021.* Geraadpleegd van: https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/jaarverslag_ap_2021.pdf

[DLAP21] DLA Piper (2021, 19 januari). *Nederland tweede van Europa in aantal gemelde datalekken sinds invoering AVG.* Geraadpleegd van: https://www.dlapiper.com/en-nl/news/2021/01/nederland-tweede-van-europa-in-aantal-gemelde-datalekken-sinds-invoering-avg

[EC21] European Commission (2021). *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* Geraadpleegd van: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

[ICTM18] ICT-Magazine (2018, 16 oktober). *Onderzoek KPMG: Nederlander nauwelijks bekend met nieuwe privacyrechten.* Geraadpleegd van: https://www.ictmagazine.nl/onderzoek-kpmg-nederlander-nauwelijks-bekend-met-nieuwe-privacyrechten/

[Meel] Van Meel, M. & Remmits, Y. (z.d.). *Risico's van algoritmes en toenemende vraag naar ethiek: Deel 4 - De burger en klant centraal bij het gebruik van algoritmes* [KPMG Blog]. Geraadpleegd van: https://home.kpmg/nl/nl/home/topics/artificial-intelligence/vertrouwen-in-algoritmes/risicos-van-algoritmes-en-toenemende-vraag-naar-ethiek.html

[KPMG18] KPMG (2018). *Een beetje privacy graag.* [Rapport op te vragen bij KPMG.]

[KPMG21] KPMG (2021, oktober). *Meer zorgen over privacy: Het resultaat van ons privacy onderzoek onder consumenten.* Geraadpleegd van: https://assets.kpmg/content/dam/kpmg/nl/pdf/2021/services/meer-zorgen-over-privacy-whitepaper.pdf

[MBZK21] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2021, juli). I*mpact Assessment Mensenrechten en Algoritmes.* Geraadpleegd van: https://open.overheid.nl/documenten/ronl-c3d7fe94-9c62-493f-b858-f56b5e246a94/pdf

[Ober19] Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan,S. (2019m 25 oktober). Dissecting racial bias in an algorithm used to manage the health of populations. *Science, 366*(6464), 447-453, Geraadpleegd van: https://www.science.org/doi/10.1126/science.aax2342

Over de auteurs

Marijn Bakker is manager bij KPMG Cyber & Privacy. Zij houdt zich bezig met AVG-implementatie- en optimalisatietrajecten, privacy-audits en -assessments en de implementatie van privacy tooling zoals OneTrust. Marijn heeft een master in Internet, Intellectueel Eigendom en IT-recht van de Vrije Universiteit in Amsterdam en een master in Ondernemingsrecht van de Universiteit Leiden.

Sterre Stolk was privacy consultant bij KPMG Nederland en is nu werkzaam als senior privacy-adviseur in de publieke sector. Bij KPMG hield zij zich bezig met diverse privacy-gerelateerde opdrachten die veelal verband houden met complexe technologische vraagstukken. Sterre heeft een master in Internet, Intellectueel Eigendom en IT-recht van de Vrije Universiteit in Amsterdam.