

AI-HANDBOEK VOOR EUROPESE NOTARISSEN



Dit document is opgesteld om het denken over artificiële intelligentie binnen het Europese notariaat te stimuleren. Het is uitsluitend bedoeld voor intern gebruik binnen het CNUE-netwerk en is niet bedoeld voor publieke verspreiding. Dit document is oorspronkelijk in het Engels gepubliceerd. Voor verduidelijking of bij vragen wordt verwezen naar de oorspronkelijke Engelse tekst. Deze Nederlandse vertaling is op verzoek van KNB uitgebracht.

Inhoudsopgave

I.	Inleiding en doel van het handboek	5
II.	Begrippenlijst	7
1.	Algemene begrippen	7
2.	Begrippen met betrekking tot gegevens en machine learning	8
3.	Soorten en belangrijkste toepassingen van AI	12
4.	Begrippen met betrekking tot de soorten en het gebruik van AI-systemen	16
5.	Belangrijkste deelnemers aan het AI-ecosysteem	16
6.	Kwesties en verschijnselen met betrekking tot AI	17
7.	Belangrijkste juridische bronnen met betrekking tot AI	19
III.	Mogelijke manieren van AI-gebruik door notarissen	20
1.	Algemene inzichten	20
2.	Algemene voordelen van het gebruik van AI	20
3.	Specifieke manieren van AI-gebruik door het notariaat	20
4.	Implementatie van AI-oplossingen door het notariaat	22
	<i>Belangrijkste conclusies</i>	23
IV.	Toepasselijkheid van de EU Artificial Intelligence Act	24
1.	Algemene inzichten en tijdlijn	24
2.	Persoonlijke en territoriale reikwijdte	24
3.	Het risicocategorisatiesysteem	25
4.	Categorisering van (potentiële) notariële AI-oplossingen onder de AI Act	25
5.	Wat te doen als een notarieel AI-systeem in de categorie hoog risico valt?	30
	<i>Belangrijkste conclusies</i>	32
V.	Data en artificiële intelligentie	33
1.	Het belang van data voor AI	33
2.	Kaders voor datagovernance	33
3.	AI-trainingsproces met verschillende data	33
4.	De risico's van aangetaste data en kenmerken van geschikte data	34
5.	Interne notariële data en externe databronnen	34
6.	Data in prompts en feedbackloops – de menselijke rol bij het verbeteren van data	35
	<i>Belangrijkste conclusies</i>	36
VI.	Bescherming van persoonsgegevens en artificiële intelligentie	37
1.	Algemene inzichten	37
2.	AVG en de AI Act	37
3.	Verschillende wetgeving – verschillende rollen	38
4.	AVG-beginselen bij AI-gebruik door notarissen	39
5.	Rechten van de betrokkene bij AI-gebruik door notarissen	41
6.	AVG en ontwikkeling van notariële AI-systemen	41
7.	Notariële AI buiten het toepassingsgebied van de AVG	43
8.	Gegevensbeschermingseffect-beoordeling en effectbeoordeling van fundamentele rechten	44
	<i>Belangrijkste conclusies</i>	46

VII. Bescherming van vertrouwelijke gegevens	48
1. Vertrouwelijke gegevens in notariële activiteiten	48
2. Problemen met gegevensinvoer in AI-systemen	48
3. Oplossingen om schending van het beroepsgeheim te voorkomen	49
<i>Belangrijkste conclusies</i>	50
VIII. AI-bias en -hallucinatie	51
1. Oorzaken en gevolgen van AI-bias	51
2. Identificatie en beperking van bias (de-biasing)	52
3. Oorzaken en effecten van AI-hallucinatie	52
4. Beperken van AI-hallucinatie	53
<i>Belangrijkste conclusies</i>	54
IX. Transparantie en verklaarbaarheid van AI-systemen	55
1. Algemene inzichten	55
2. AI-transparantie en -verklaarbaarheid – de belangrijkste verschillen	55
3. Methoden voor transparantie en verklaarbaarheid	56
4. Transparantieverplichtingen in de AI Act	56
5. Black box AI vs. white box AI	56
6. Het belang van AI-transparantie en -verklaarbaarheid in het notariaat	57
<i>Belangrijkste conclusies</i>	59
X. Human-in-the-loop—de rol van de notaris in een AI-gedreven wereld	60
1. Mogelijkheden en beperkingen van AI	60
2. De rol van notarissen in een wereld met AI	60
3. Werken met AI	61
<i>Belangrijkste conclusies</i>	63
XI. Intellectueel eigendom en artificiële intelligentie	64
1. Algemene inzichten – Identificatie van de relevante IP-rechten in notarieel-AI-verband	64
2. Auteursrecht op notariële akten, rechtsinstrumenten en databanken voor AI	64
3. Uitzondering en beperking van tekst- en datamining voor AI-training	65
4. Auteursrechtelijke bescherming van AI-output	66
<i>Belangrijkste conclusies</i>	68
XII. Kant-en-klare, intern ontwikkelde en extern geleverde AI-systemen	69
1. ‘Kant-en-klare’ AI-systemen	69
2. Voordelen en moeilijkheden van intern ontwikkelde AI-oplossingen voor notarissen	69
3. Notariële AI-systemen geleverd door externe dienstverleners (AI as a Service)	70
<i>Belangrijkste conclusies</i>	73
XIII. Basics of AI cybersecurity	74
1. Algemene inzichten	74
2. Beveiligingsrisico's voor AI-systemen en mogelijke tegenmaatregelen	74
3. Europese regelgeving voor AI-cyberveiligheid	75
4. AI-cyberveiligheid en het notariaat	77
<i>Belangrijkste conclusies</i>	78

I. Inleiding en doel van het handboek

Ook al is artificiële intelligentie (AI) in verschillende vormen al lang bekend, in het vorige decennium is het een zichtbaar ontwrichtende technologie geworden. De grote hoeveelheid digitale gegevens die elke dag wordt geproduceerd en de voorheen onvoorstelbare rekenkracht hebben samen bijgedragen aan de groei van AI van eenvoudige software tot een extreem krachtig hulpmiddel, dat processen, beroepen en de manier waarop mensen hun leven leiden kan transformeren. Nieuwe AI-oplossingen dringen razendsnel ons leven binnen (bijv. de generatieve AI-modellen), die nieuwe fenomenen en kansen creëren, maar ook nieuwe risico's met zich meebrengen. Het is dan ook niet verwonderlijk dat de wetgever van de Europese Unie deze technologie uitgebreid wilde reguleren met het aannemen van de Artificial Intelligence Act (AI Act); de eerste reeks wettelijke bepalingen die wereldwijd op dit gebied van toepassing is.

Tegenwoordig wordt AI op grote schaal toegepast in het dagelijks leven en bij de uitoefening van een groot aantal beroepen. De juridische sector vormt hierop geen uitzondering: advocaten, rechters, bedrijfsjuristen en juristen van de overheid maken al gebruik van algemene en speciale AI-oplossingen. Het gebruik van AI levert voordelen op, zowel in het dagelijks leven als op professioneel gebied. Tegelijkertijd is AI, zoals hierboven beschreven, niet zonder risico's en gevaren, waarmee sterk rekening moet worden gehouden. Vaak—en niet zonder reden—nemen juridische professionals een houding aan van angst voor deze risico's en gevaren, waardoor ze terughoudend zijn in het gebruik van AI.

Dit handboek is bedoeld om Europese notarissen dichterbij AI-technologie te brengen door de mogelijke manieren te presenteren waarop de vele AI-oplossingen die momenteel bestaan, gebruikt kunnen worden. Tegelijkertijd belicht dit handboek de belangrijkste, reeds geïdentificeerde risico's van dergelijk gebruik, om de rechtszekerheid en het hoge niveau van professionele diensten te garanderen die notarissen gewend zijn te leveren, zelfs wanneer deze technologie niet wordt ingezet.

De toepassing van de informatie en verklaringen in het handboek is geheel vrijwillig. Het staat notariële organisaties en individuele notarissen vrij om verschillende stap-

pen en benaderingen te volgen, afhankelijk van hun eigen beslissingen en de wetten die op hen van toepassing zijn.

Hoewel het doel van het handboek niet is om notarissen experts te maken op het gebied van AI-technologie, bevat dit document een uitgebreide en thematische begrippenlijst waarin de belangrijkste technologische termen die verband houden met AI en waarmee notarissen in verschillende omstandigheden kunnen worden geconfronteerd, duidelijk worden uitgelegd. Zo kunnen notarissen een multidisciplinaire aanpak hanteren door technologie en recht op een nog complexer en verfijnder niveau te combineren dan in het verleden.

In deze inleiding moet al worden benadrukt dat AI in zijn huidige vorm geen vervanging kan zijn voor een notaris. AI is een technologie die kan worden gebruikt om notarissen te helpen bij hun dagelijkse werk, en als dit op de juiste manier wordt gedaan, kan het leiden tot een hogere kwaliteit van dienstverlening en een grotere efficiëntie, waardoor notarissen zich meer kunnen concentreren op moeilijke juridische zaken dan op routinetaken.

Het Handboek heeft ook tot doel om lezers inzicht te geven in de potentiële voordelen van AI voor notarissen en notariële organisaties. Hoewel de basisprincipes van het notariaat vergelijkbaar of hetzelfde zijn in de 22 landen van de EU die het notariële systeem van het Latijnse type hebben (en die ook lid zijn van de Raad van Notarissen van de Europese Unie – CNUe), kunnen er ook aanzienlijke verschillen zijn, afhankelijk van de juridische, economische en sociale omstandigheden en de historische ontwikkeling van de betreffende landen. Dit kan ook van grote invloed zijn op het gebruik van AI-toepassingen. Daarom wil het handboek 'notarieel neutraal' zijn, wat betekent dat de informatie in dit document geschikt en nuttig is voor de 22 staten. Landspecifieke informatie (bijvoorbeeld over specifieke AI-oplossingen die al in gebruik zijn bij notarissen in een bepaalde staat) en voorstellen maken geen deel uit van dit handboek. Er wordt alleen naar verwezen als het nodig is om dieper op het onderwerp in te gaan.

Hoewel het handboek niet tot doel heeft Europese AI-systemen voor notarissen op te zetten die in de 22 notariaten van Europa worden toegepast, kunnen de ver-

klaringen in het handboek voor dergelijke AI-systemen worden gebruikt indien alle leden van de CNUE besluiten een dergelijk systeem op te zetten.

In dit document worden de risico's en gevaren van het gebruik van AI in detail beschreven en worden mogelijke oplossingen voorgesteld om ze te beperken of—indien mogelijk—te vermijden. Aangezien de bovengenoemde AI Act onafhankelijk van het beroep van de ontwikkelaar of gebruiker van toepassing is, worden de bepalingen die moeten of kunnen worden toegepast op het notariaat als AI-ontwikkelaar/gebruiker ook geïdentificeerd en geanalyseerd in het Handboek. Dit geeft het notariaat de gelegenheid om zich ruim van tevoren voor te bereiden op de naleving van de bepalingen van de AI Act die vanaf augustus 2026 volledig van toepassing zal zijn.

Tot slot weerspiegelt de huidige versie van het handboek de stand van de technologie waarvan de gerelateerde informatie openbaar werd tot 17 februari 2025 en de wettelijke bepalingen die van kracht waren op het moment van goedkeuring door de CNUE. Door de extreem snelle ontwikkeling van AI moet het handboek echter regelmatig worden bijgewerkt.

Tot slot weerspiegelt de huidige versie van het handboek de stand van de technologie waarvan de gerelateerde informatie openbaar werd tot 17 februari 2025 en de wettelijke bepalingen die van kracht waren op het moment van goedkeuring door de CNUE. Door de extreem snelle ontwikkeling van AI moet het handboek echter regelmatig worden bijgewerkt.

II. Begrippenlijst

Deze thematische begrippenlijst is bedoeld om de meest gebruikte termen met betrekking tot kunstmatige intelligentie (AI) uit te leggen en te zorgen voor een eenvoudig begrip van de vaak technische woordenschat die nodig is om AI te begrijpen. De begrippenlijst volgt niet de alfabetische volgorde van de woorden. De inhoud is gegroepeerd rond de begrippen die in een vergelijkbare context voorkomen en/of een logische volgorde volgen van algemeen naar meer bijzonder. De termen in de begrippenlijst staan in de tekst van het handboek onder de verschillende hoofdstukken. Daarom worden ze later niet apart gedefinieerd, maar hyperlinks helpen de lezer terug te gaan naar het relevante deel van de begrippenlijst.

Het is belangrijk op te merken dat — met enkele aangegeven uitzonderingen — de onderstaande definities geen officiële definities zijn. Verschillende specialisten hebben verschillende visies en opvattingen over AI-gerelateerde termen. Bovendien verandert en evolueert de werkelijke betekenis van de termen in de loop der tijd, afhankelijk van nieuwe technologische ontwikkelingen, wetgeving en gebruikssituaties. Het doel van de begrippenlijst is dan ook niet om officieel definities te formuleren, maar om een goed begrip te geven van de termen waarmee notarissen te maken krijgen in een steeds meer door AI gestuurde wereld.

De voorbeelden in deze begrippenlijst zijn bedoeld om de definities in een praktische context te plaatsen, waarbij de nadruk ligt op het notariaat. Het hoeft niet om echte gebruikssituaties te gaan. Onder voorbehoud van toestemming van de regelgevende instanties of in geval van een verbod, geven ze echter gevallen weer die zich al hebben voorgedaan of die zich in de toekomst zouden kunnen voordoen binnen het notariaat. Bovendien leggen de voorbeelden een specifieke term uit zonder specifiek alle potentiële risico's eromheen te belichten. Deze zijn te vinden in verschillende hoofdstukken van dit handboek.

1. Algemene begrippen

a) Artificiële intelligentie (AI):

Artificiële intelligentie is een tak van de computerwetenschap met algoritmen die onafhankelijk van menselijke

tussenkomen beslissingen, voorspellingen, inhoud en aanbevelingen kunnen doen in de vorm van output. AI kan eenvoudige en zelfs complexe taken uitvoeren die voorheen alleen door mensen konden worden uitgevoerd.

Ondanks de benaming wordt AI niet beschouwd als intelligentie in de menselijke betekenis van het woord. AI kan niet denken en de taken die het uitvoert begrijpen zoals mensen dat doen. Bovendien kan het op dit moment situaties niet goed in context plaatsen en kan het evenmin abstracties maken. AI-systemen kunnen uitblinken in specifieke taken, maar zijn niet in staat om dit vermogen over te dragen op taken waar ze niet voor geprogrammeerd zijn.

De term 'AI' heeft een brede betekenis, maar wordt—in de wetenschappelijke literatuur, door leken en ook in dit handboek—gebruikt voor software die aan de bovenstaande beschrijving van 'artificiële intelligentie' (AI) voldoet. Zoals hieronder wordt aangegeven, omvat AI verschillende technologieën. Daarom wordt AI gebruikt als overkoepelende term voor verdere discussies.

b) AI-systeem:

“Een op een machine gebaseerd systeem dat is ontworpen om te werken met verschillende niveaus van autonomie en dat na zijn inzet aanpassingsvermogen kan vertonen en dat, voor expliciete of impliciete doelstellingen, uit de input die het ontvangt afleidt hoe het outputs kan genereren zoals voorspellingen, content, aanbevelingen of beslissingen die fysieke of virtuele omgevingen kunnen beïnvloeden” (definitie AI Act, artikel 3, lid 1).

AI-systemen integreren een of meer AI-model(len) om specifieke taken uit te voeren. Het AI-systeem is het operationele kader. Naast AI-modellen omvatten AI-systemen de volgende hoofdcomponenten: gegevensverzameling en -verwerking (voor het verzamelen en voorbereiden van trainingsdata voor het model), gebruikersinterface (waarmee gebruikers interageren met het systeem, bijvoorbeeld toepassingen) en infrastructuur (hardware en software die nodig zijn om het systeem te laten werken).

Voor verdere (niet-bindende) richtsnoeren over de definitie van “AI-systeem”, zie de *Goedkeuring van de inhoud*

van de ontwerp Mededeling van de Commissie – Commissie Richtlijnen voor de definitie van AI-systemen vastgesteld bij Verordening (EU) 2024/1689 (AI Act)'.
(overgenomen uit de Mededeling van de Commissie)

c) AI-model:

Een AI-model is het belangrijkste onderdeel van een AI-systeem dat een algoritme bevat. Het is een wiskundige of statistische voorstelling van een specifiek probleem, ontwikkeld uit data. AI-modellen worden getraind om patronen te herkennen, voorspellingen te doen of beslissingen te nemen op basis van data en een precieze taak uit te voeren.

2. Begrippen met betrekking tot gegevens en machine learning

a) AI-datagovernance:

AI-datagovernance richt zich op het beheer van de gegevens die worden gebruikt door AI-systemen en houdt zich bezig met vraagstukken over gegevenskwaliteit, integriteit, rechtmatigheid, privacy, beveiliging en de bruikbaarheid van de gegevens door de betreffende aanbieder/gebruiker. Binnen het kader voor datagovernance stelt de aanbieder/gebruiker beleid, normen en procedures op voor de verzameling, opschoning, annotatie, opslag, analyse en gebruik van gegevens met als doel te voldoen aan zowel wettelijke als ethische regels.

Naast het ondersteunen van de behoeften van de aanbieder/gebruiker, helpt een geschikt kader voor datagovernance bij het beperken van risico's (bijv. inbreuken op persoonsgegevens, bias en discriminatie) en draagt bij aan de transparantie van de ontwikkeling en het gebruik van AI, waardoor het vertrouwen in het kader toeneemt. Binnen het kader voor datagovernance worden zowel organisatorische rollen en verantwoordelijkheden als technische stappen vastgelegd en het kader moet regelmatig worden gecontroleerd en bijgewerkt om gelijke tred te houden met de veranderingen in wettelijke regels en technologische ontwikkelingen.

Voorbeeld voor het notariaat: Een notaris gebruikt een AI-oplossing voor de automatische verwerking van grote juridische documenten. Een goed kader voor AI-datagovernance zorgt ervoor dat de gegevens die hij/zij gebruikt, zoals persoonsgegevens (bijv. de naam van de cliënt) en niet-persoonsgebonden vertrouwelijke

gegevens (bijv. handelsgeheimen van de cliënt), veilig worden bewaard en dat de verwerking ervan voldoet aan de relevante wettelijke bepalingen. Dit omvat onder andere regels over de personen met recht van toegang tot de gegevens, de toegestane duur van de opslag en de manieren van bescherming.

b) Tekst- en datamining (TDM):

TDM is een geautomatiseerd proces voor het digitaal selecteren en analyseren van grote hoeveelheden inhoud (tekst en/of gegevens) met behulp van verschillende computergebaseerde en statistische technieken (meestal natuurlijke taalverwerking) met als doel verborgen patronen, trends, relaties en andere nuttige informatie te ontdekken..

TDM kan worden onderverdeeld in de volgende twee subcategorieën:

- Datamining is het computergebaseerde proces van het ontdekken en extraheren van patronen en kennis uit gestructureerde gegevens.
- Tekstmining doet hetzelfde, maar dan met ongestructureerde ruwe (tekst)gegevens. Tekstmining kan worden beschouwd als een specifieke vorm of de voorbereidingsfase van datamining, waarin de ongestructureerde tekstuele gegevens eerst worden omgezet in gestructureerde gegevens die vervolgens efficiënter kunnen worden geanalyseerd. Daarom worden de begrippen tekst- en datamining beide vaak gebruikt.

TDM kan dienstverleners helpen om onder andere voorspellingen te doen en betere beslissingen te nemen.

Voorbeeld voor het notariaat: Een beroepsorganisatie wil documenten over onroerend goed analyseren om huidige trends te ontdekken en mogelijke toekomstige problemen in de sector te voorspellen. De organisatie kan TDM gebruiken om een enorme hoeveelheid relevante documenten te analyseren om patronen en trends te identificeren en voorspellingen te doen. Dit helpt de beroepsgroep om haar acties te stroomlijnen en zich voor te bereiden op toekomstige situaties.

c) Trainingsgegevens—validatiegegevens—testgegevens:

‘Trainingsgegevens zijn gegevens die worden gebruikt voor het trainen van een AI-systeem door het aanpassen van de leerbare parameters’ [definitie AI Act, artikel 3, punt 29]. Trainingsgegevens worden gebruikt om het AI-model te trainen door te leren vooraf bepaalde taken uit te voeren (bijv. suggesties doen voor beslissingen). Trainingsgegevens zijn meestal afkomstig van menselijke input, specifieke trainingsdatasets of van machines (bijv. sensoren). Afhankelijk van het doel van het AI-systeem kunnen de trainingsdata divers zijn: tekst (bijv. wetteksten, contracten), beeld of video (bijv. voor gezichtsherkenning), menselijke spraak (bijv. voor dicteren) en sensordata (bijv. voor biometrische verificatie). Trainingsgegevens kunnen gelabeld of ongelabeld zijn. De eerste gebruikt labels die helpen bij de identificatie van vergelijkbare objecten, patronen, emoties, etc., de tweede heeft geen labels.

Validatiedata: data die wordt gebruikt om het getrainde AI-systeem te evalueren en voor het afstemmen van de niet-leerbare parameters en het leerproces af te stemmen om onder meer underfitting of overfitting te voorkomen.’ [definitie AI Act, Artikel 3, lid 30]. Op basis van de validatiegegevens wordt de training van het AI-systeem beoordeeld en wordt het beste model gekozen voor de betreffende taak. De validatiefase biedt ook de gelegenheid om het model te verfijnen en verder te ontwikkelen.

‘Testdata is data die wordt gebruikt voor een onafhankelijke evaluatie van het AI-systeem om de verwachte prestaties van dat systeem te bevestigen voordat het op de markt komt of in gebruik wordt genomen.’ [definitie AI Act, artikel 3, lid 31]. Testdata bepaalt hoe goed het model daadwerkelijk is. Als een bepaalde benchmark niet wordt gehaald moet er betere trainingsdata komen en moet de training opnieuw worden gestart. Als het model de benchmark haalt, kan het worden goedgekeurd.

Om objectieve testresultaten te garanderen, is het niet toegestaan om de validatie- en testdata samen te voegen. De testdata moeten dicht bij de echte wereld liggen en de tests moeten altijd worden uitgevoerd met data die nog niet eerder is gezien.

Voorbeeld voor het notariaat: Een beroepsorganisatie ontwikkelt een AI-oplossing om notarissen te helpen bij het opsporen van ontbrekende clausules in

hun akten. Het AI-model wordt getraind op een grote hoeveelheid adequaat voorbereide (bijv. geanonimiseerde) contracten uit het verleden (trainingsdata). Na de training van het systeem krijgt het model een dataset (validatiedata) om zijn eerste evaluatie uit te voeren. Tijdens deze fase worden kleine onnauwkeurigheden van het model gedetecteerd, die worden opgelost voordat het model naar de testfase gaat. Tijdens het testen ontvangt het model totaal andere contracten dan die gebruikt zijn in de validatiefase (testdata) om de nauwkeurigheid van het model te bevestigen voordat het door de beroepsgroep wordt gebruikt. Nadat de AI-oplossing de test heeft doorstaan, is deze klaar voor gebruik door notarissen.

d) Synthetic data:

Synthetische data is kunstmatige data die wordt gegenereerd uit oorspronkelijke data en de kenmerken en structuur ervan reproduceren. Synthetische data bootst echte data na. In de praktijk helpt het machine learning algoritmen te trainen als de werkelijke data beperkt of gevoelig is. Het gebruik van synthetische data is vooral nuttig om problemen met de bescherming van persoonsgegevens te vermijden tijdens het trainen van het AI-model.

Voorbeeld voor het notariaat: Voorbeeld voor het notariaat: De dataset die beschikbaar is voor een beroepsorganisatie om zijn AI-model te trainen voor hulp bij het opstellen van contracten (in ontwikkeling) bevat persoonsgegevens die moeten worden gemaakt. Echter, denkend aan de gevaren van de-anonimisering (heridentificatie) besluit de beroepsorganisatie om synthetische data te genereren (bijv. valse contracten met correcte juridische informatie maar zonder persoonsgegevens) op basis van echte data om het AI-model te trainen zonder de privacy en persoonsgegevens van cliënten in gevaar te brengen.

e) Persoonsgegevens, niet-persoonsgebonden gegevens:

‘Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (‘de betrokkene’); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elemen-

ten die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. [AVG definitie, artikel 4, lid 1]

Niet-persoonsgebonden gegevens zijn alle gegevens die niet onder de vorige categorie vallen.

Voorbeeld voor het notariaat: Persoonsgegevens zijn onder andere de naam, geboortedatum en -plaats, adres en persoonlijke identificatienummers van cliënten. Notariële akten bevatten ook een grote verscheidenheid aan niet-persoonsgebonden gegevens, zoals de aankoopprijs, het kapitaal van de op te richten onderneming, de rentevoeten, enz.

f) Pseudonimisering en gepseudonimiseerde gegevens:

‘Pseudonimisering: het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld’ [AVG definitie, artikel 4, lid 5]. De originele gegevens worden vervangen door een pseudoniem. Pseudonimisering is omkeerbaar en maakt latere heridentificatie mogelijk. Het is een methode voor gegevensbescherming die wordt aanbevolen in de AVG.

Voorbeeld voor het notariaat: Om de privacy en persoonsgegevens van cliënten in geautomatiseerde systemen te beschermen, vervangt de notaris/notariële organisatie persoonsgegevens door pseudoniemen. De naam van de cliënt wordt bijvoorbeeld vervangen door een unieke identificatiecode, waardoor de echte gegevens alleen kunnen worden opgevraagd door degenen die de benodigde rechten (sleutel) hebben.

g) Anonimisering en geanonimiseerde (gede-identificeerde) gegevens:

Als de gegevens worden geanonimiseerd, worden ze in principe onherstelbaar gewijzigd, wat betekent dat de achterliggende individuen niet meer (direct of indirect) kunnen worden geïdentificeerd, waardoor de AVG niet meer

van toepassing is. Het de-identificatieproces omvat het versleutelen, maskeren, generaliseren, verstoren of verwijderen van zowel de directe als de indirecte identificatoren.

Voorbeeld voor het notariaat: Een beroepsorganisatie wil een AI-systeem ontwikkelen voor de aangesloten notarissen. Vóór het trainen van het systeem, anonimiseert de beroepsorganisatie de persoonsgegevens van de cliënten in het relevante trainingsmateriaal. Dit betekent het verwijderen van namen, geboorteplaatsen en geboortedata, adressen, persoonlijke identificatiemiddelen en alle andere gegevens op basis waarvan de betreffende natuurlijke persoon kan worden.

h) De-anonymisation (re-identification):

Persoonsgegevens de-anonimiseren is de methode voor het matchen van geanonimiseerde gegevens met openbaar beschikbare informatie, of aanvullende gegevens, met behulp van technologie om de persoon van wie de gegevens zijn te identificeren. De-anonisering keert het proces van anonimiseren. Iom. Uit de beschikbare dataset kan informatie worden gehaald om de identiteit van een persoon te achterhalen.

Voorbeeld voor het notariaat: Als het mogelijk is om een verband te leggen tussen de geanonimiseerde gegevens in een notariële akte en openbaar beschikbare informatie (bijvoorbeeld uit het elektronische kadaster), kan de persoon in kwestie mogelijk ook de persoon achter de specifieke transactie identificeren. Daarom vereist dit risico dat het notariaat ook bij de ontwikkeling en het gebruik van AI uiterst omzichtig te werk gaat.

i) Gegevensverzameling/acquisitie

Gegevensverzameling/acquisitie is het proces van het verzamelen van ruwe gegevens voor AI-training. De verzamelde gegevens moeten van een grote hoeveelheid, hoge kwaliteit en representatief genoeg zijn voor het doel van het AI-model. Het verzamelen van gegevens uit de echte wereld is de meest ideale oplossing, maar als er onvoldoende van dergelijke gegevens zijn, kan synthetische data data helpen om gaten in de gegevens op te vullen.

Voorbeeld voor het notariaat: Voor de training van een notarieel AI-systeem verzamelt de ontwikkelkamer de benodigde gegevens uit verschillende bronnen, zoals databanken, openbare registers, juridische literatuur en,

afhankelijk van de wettelijke toestemming en indien de notaris die ze opstelt geen bezwaar heeft, contracten en andere notariële akten.

j) Labelen / annotatie van gegevens:

Het proces van het geven van tags/labels aan de trainingsdata of een deel daarvan. Deze oplossing wordt meestal gebruikt voor supervised learning.

Voorbeeld voor het notariaat: Een machine of een team van experts plaatst labels op trainingsdata in documenten om de belangrijkste informatie te identificeren, zoals de aankoopprijs, de rentevoet of de clausules over het rechtsgebied en de toepasselijke wetgeving. Dit helpt het AI-systeem om dezelfde of vergelijkbare soorten gegevens in andere documenten te herkennen.

k) Gegevensopschoning

Het proces van reageren op problemen met gegevens, waaronder bijvoorbeeld het corrigeren van fouten, het verwijderen van irrelevante, dubbele of inconsistente gegevens en het oplossen van het probleem van onvolledige datasets.

Voorbeeld voor het notariaat: Vóór het trainen van het AI model moet de ontwikkelkamer de verzamelde gegevens opschonen. Dit kan bijvoorbeeld zijn het verwijderen uit de dataset van akten die zijn opgesteld op basis van wetgeving die niet meer van kracht is, of gegevens die meerdere keren onnodig voorkomen in de dataset.

l) Training van artificiële intelligentie:

De activiteit van het invoeren van trainingsdata in het AI-algoritme.

Voorbeeld voor het notariaat: De ontwikkelkamer voert gegevens van verschillende bronnen in het systeem in, zodat het algoritme zijn vooraf bepaalde taak kan uitvoeren.

m) Machine learning (ML):

Machine learning is een methode van training van AI-modellen. Met ML leren algoritmen van data zonder expliciet geprogrammeerd te worden.

Voorbeeld voor het notariaat: Door labels, patronen en correlaties te gebruiken in de data voor het AI-systeem, kan het model zelf 'leren' en wordt het na verloop van tijd steeds beter in het identificeren van kenmerken in contracten en in het verbeteren, wijzigen, etc. van specifieke contracten, wat de uitvoerende notaris helpt bij het opstelproces.

Er bestaan drie hoofdtypen ML-methoden:

- **Supervised learning:** het AI-model wordt gevoed met gelabelde gegevens. De labels zijn de output die de AI moet leren produceren, net zoals in de fysieke wereld wanneer leerlingen leren van de voorbeelden die de leraar geeft en deze kennis teruggeven bij het examen. Een AI die is getraind met supervised learning is in staat om ongelabelde gegevens correct te herkennen. Voorbeelden van toepassingen van supervised learning zijn onder andere classificatie, spraakherkenning and sentimentanalyse.

Voorbeeld voor het notariaat: De notaris kan AI-oplossingen gebruiken die zijn getraind om hun handelingen te classificeren op basis van eerder gelabelde gegevens. Deze oplossing maakt het bijvoorbeeld makkelijker om documenten op een later punt terug te vinden.

- **Unsupervised learning:** het AI-model wordt gevoed met ongelabelde gegevens zonder enige hulp om zelf patronen en correlaties te vinden. Een AI-model dat op deze manier is getraind, kan vaak ongebruikelijke patronen vinden en identificeren om efficiëntere oplossingen te bieden. Unsupervised learning wordt bijvoorbeeld gebruikt voor het extraheren van kenmerken.

Voorbeeld voor het notariaat: Na het vinden van patronen en correlaties in de trainingsdata kan de AI-oplossing de notaris helpen om een samenvatting te maken van de informatie in grote hoeveelheden documenten, waardoor de belangrijkste punten van de specifieke documenten sneller worden geïdentificeerd.

- **Reinforcement learning:** het AI-model wordt gevoed met ongelabelde gegevens zonder enige hulp om zelf patronen en correlaties te vinden. Een AI-model dat op deze manier is getraind, kan vaak ongebruikelijke

kelijke patronen vinden en identificeren om efficiëntere oplossingen te bieden. Unsupervised learning wordt bijvoorbeeld gebruikt voor het extraheren van kenmerken.

Voorbeeld voor het notariaat: Een AI-oplossing die wordt getraind met reinforcement learning krijgt, bijvoorbeeld voor het verifiëren van de volledigheid van de notariële akten, een 'beloning' (positieve feedback) als de output correct is (dus als de AI een correcte clausule voorstelt om toe te voegen of correct detecteert dat het contract volledig is) en een 'straf' (negatieve feedback) als de output incorrect is. Dankzij deze methode wordt het AI-model steeds nauwkeuriger en betrouwbaarder.

n) Neural network:

Een neural network is een machine learning model dat gebruikmaakt van processen die de manier nabootsen waarop biologische neuronen in het menselijk brein samenwerken om verschijnselen te identificeren, opties af te wegen en tot conclusies te komen. Neural networks bestaan uit lagen van knooppunten (die kunstmatige neuronen zijn): een inputlaag, een of meer verborgen lagen en een outputlaag. De knooppunten (nodes) zijn met elkaar verbonden en hebben hun bijbehorende gewichten (weights) en drempels (thresholds). Als de output van een knooppunt boven de gespecificeerde drempelwaarde ligt, wordt dat knooppunt geactiveerd en stuurt het gegevens naar de volgende laag van het netwerk. Een van de bekendste voorbeelden van een neural network is het zoekalgoritme van Google.

o) Deep learning:

Een neural network dat uit meer dan drie lagen bestaat, wordt beschouwd als een deep learning algoritme. Deep learning is dus een soort machine learning waarbij gebruik wordt gemaakt van kunstmatige neural networks met meerdere lagen om complexe patronen te leren in grote hoeveelheden data. Deep learning wordt gebruikt in toepassingen zoals spraakherkenning en natuurlijke taalverwerking.

p) Data poisoning:

Een type cyberaanval waarbij een trainingsdataset gebruikt door een AI-model opzettelijk wordt aangetast om de werking van het model te manipuleren. Dit kan op

verschillende manieren gedaan worden, zoals het injecteren van valse informatie in de trainingsdataset, of het wijzigen of (deels) verwijderen van de dataset. Het mogelijke gevolg van data poisoning of 'data-vergiftiging' is een onbetrouwbare en onnauwkeurige uitvoer van het AI-systeem. Wanneer een inbreuk wordt gedetecteerd moet deze worden getraceerd en moet de dataset worden hersteld. In sommige gevallen moet het model volledig opnieuw worden getraind

Voorbeeld voor het notariaat: In de trainingsdataset van een AI-systeem dat door notarissen wordt gebruikt om de naleving van de geldende wet te detecteren, introduceert iemand opzettelijk gegevens over verouderde wetteksten ('vergiftigt' de trainingsdataset). Als gevolg daarvan geeft de AI onjuiste suggesties op basis van wettelijke bepalingen die niet meer van kracht zijn.

3. Soorten en belangrijkste toepassingen van AI

a) Op regels gebaseerde systemen:

In de vroegste versies van toepassingen voor natuurlijke taalverwerking werden 'als-dan' stellingen geformuleerd die afhankelijk waren van een vooraf gedefinieerde set expliciete regels. Op regels gebaseerde systemen kunnen alleen antwoorden geven op specifieke gebruikersinput in specifieke domeinen, waardoor hun mogelijkheden beperkt zijn in vergelijking met machine learning systemen doordat ze geen complexe situaties aankunnen en zich daaraan kunnen aanpassen.

Voorbeeld voor het notariaat: Een beroepsorganisatie ontwikkelt een chatbot om cliënten te helpen basisinformatie over de wet te krijgen. Als er bijvoorbeeld de vraag komt of een bepaald type contract geldig kan worden opgesteld zonder notariële tussenkomst, kan de op regels gebaseerde chatbot een duidelijk 'ja' of 'nee' antwoord geven.

Het voordeel van op regels gebaseerde systemen is echter de transparantie en daarmee het gemak van interpretatie van het besluitvormingsproces door het systeem. Op regels gebaseerde systemen zijn efficiënt in het omgaan met goed gedefinieerde problemen. Bovendien is het bijwerken van het systeem en het fouten oplossen eenvoudiger dan bij geavanceerde machine learning systemen.

b) AI-modellen voor algemene doeleinden (GPAI) / Foundation models

‘AI-modellen die een aanzienlijke mate van generaliteit vertonen, in staat zijn om een breed scala aan afzonderlijke taken uit te voeren en die kunnen worden geïntegreerd in een verscheidenheid aan downstreamsystemen of -toepassingen.’ [definitie AI Act, artikel 3 (63)].

Een foundation model is een deep learning model dat als basis dient voor verschillende soorten generatieve AI-toepassingen. Omdat deze modellen een breed scala aan algemene taken kunnen uitvoeren, verschillen ze van de zogenaamde ‘smalle’ AI-systemen die zich alleen richten op een specifieke taak, zoals het genereren van tekst. Voor de training van foundation models is een enorme hoeveelheid onbewerkte en ongelabelde data nodig (meestal van het internet gehaald) en ze kunnen voor verschillende taken worden gebruikt met minimale fine-tuning (extra datasets toevoegen en niet helemaal opnieuw beginnen met ontwikkelen).

Deze modellen worden beschikbaar gesteld aan downstream ontwikkelaars via API's (Application Programming Interfaces), vaak open-source. Voorbeelden van GPAI-modellen zijn GPT-4, DALL-E, Google BERT

GPAI-modellen zijn al lange tijd in het vizier van de EU-wetgever tijdens het werken aan de AI Act omdat ze de basis vormen voor een reeks toepassingen (bijv. OpenAI's basismodel GPT-4 of Microsoft's Copilot), en elke fout op GPAI-niveau kan negatieve gevolgen hebben voor de toepassingen die erop zijn gebouwd. Bovendien maken GPAI-modellen ook gebruik van 'transfer learning', wat betekent dat ze geleerde patronen van de ene taak toepassen op een andere.

c) Generatieve artificiële intelligentie (gen AI):

Generatieve AI kan op verzoek inhoud creëren, zoals samenhangende en relevante tekst, afbeeldingen, video, audio, spraak of softwarecode, op basis van de invoer van de gebruiker. Een van de meest wijdverspreide gen-AI's is ChatGPT. Gen-AI is meestal gebaseerd op foundation (GPAI) models die zijn afgestemd op een specifieke taak voor het genereren van inhoud. De meest ontwikkelde generatieve AI-modelarchitectuur is de zogenaamde transformer (GPT betekent: Generative Pre-trained Transformer) die artike-

len en artistieke werken kan genereren, dus niet alleen eenvoudige antwoorden op vragen. Transformermodellen kunnen ook getraind worden om extra hulpmiddelen te gebruiken om een bepaalde soort uitvoer te creëren.

Generatieve AI heeft ook een aantal typische negatieve kenmerken: hallucinaties waarbij er verschillende outputs zijn bij dezelfde input, het genereren van vooringenomen outputs en het gebrek aan verklaarbaarheid.

GPAI and gen AI Voorbeeld voor het notariaat: GPAI

en gen-AI voorbeeld voor het notariaat: Een beroepsorganisatie als downstream-ontwikkelaar besluit om van een vertrouwde foundation model ontwikkelaar een GPAI te integreren gebaseerd op individueel overeengekomen contractuele voorwaarden (die de naleving van de wettelijke verplichtingen van notarissen garanderen). Het model is getraind op een grote hoeveelheid juridische gegevens uit het land van de beroepsorganisatie. Na het fine-tunen van het model voor specifieke notariële doeleinden en het creëren van een goed generatieve AI-systeem binnen de specifieke beroepsorganisatie, kunnen notarissen er gebruik van maken door bijvoorbeeld automatisch de eerste concepten van hun akten te genereren.

d) Unimodale en multimodale AI:

Modaliteit verwijst naar het type gegevens dat kan worden verwerkt door AI-systemen. Dit zijn bijvoorbeeld tekst-, beeld-, audio-, video- of multimediate gegevens.

Unimodale AI-systemen kunnen slechts één type modaliteit verwerken (meestal tekst) en alleen hetzelfde type uitvoer leveren.

Multimodale AI is in staat om meerdere modaliteiten van gegevensinvoer te verwerken en dezelfde of verschillende modaliteiten van uitvoer te genereren. Een voorbeeld van een multimodaal AI-systeem is OpenAI's GPT-4V(ision) die tekst en beeld kan verwerken (zowel invoer als uitvoer). Een multimodaal AI-systeem bestaat uit talrijke unimodale neural networks.

Multimodale AI-systemen hebben een grotere hoeveelheid verschillende gegevens nodig, maar zijn in ruil daarvoor in staat om patronen en verbanden tussen verschillende soorten gegevensinvoer te herkennen en nauwkeurigere uitvoer te produceren.

Voorbeeld voor het notariaat: Een unimodale AI verwerkt grote hoeveelheden teksten die de notaris moet nakijken en maakt de eerste (geschreven) samenvatting van die teksten als output. Een multimodale AI is in staat om de concepttekst van de akte (schriftelijk formaat) en de mondeling gepresenteerde behoeften van de cliënt (audioformaat) te combineren tot een tweede ontwerp van de specifieke notariële akte.

e) Large language models (LLM's):

Large language models gebruiken deep learning-technologie, die soms honderden miljarden parameters verwerken en worden getraind op immense hoeveelheden tekst (miljarden pagina's). Ze herkennen en genereren op een menselijke manier natuurlijke taal en andere soorten inhoud om een veelheid aan taken aan te kunnen. Ze zijn in staat om samenhangende en relevante antwoorden op vragen te genereren (bijv. chatbots en virtuele assistenten), zinnen automatisch aan te vullen, documenten te vertalen, tekst samen te vatten (bijv. voor onderzoek) of content te genereren (zoals artikelen) en zelfs computercodes.

Tokens zijn de basiseenheden voor invoer en uitvoer in een LLM. Tokens vertegenwoordigen meestal woorden of tekens. Tijdens de training verwerken de LLM's de ingevoerde tekst als een opeenvolging van tokens.

LLM's leren om autonoom het volgende karakter of woord (token) in een zin te voorspellen op basis van de voorgaande woorden en context, door een waarschijnlijkheidsscore toe te kennen aan de herhaling van woorden. Het resultaat is een samenhangende en contextueel relevante tekst. Deze technologie wordt veel gebruikt in e-mails om tijdens het schrijven suggesties te doen voor het volgende woord of de volgende woorden. Tijdens het gebruik kan de prestatie van LLM's worden verbeterd door prompts gegeven door gebruikers.

LLM's worden onder andere gebruikt in natuurlijke taalverwerking en zijn bijvoorbeeld bekend van Open AI's ChatGPT of Meta's Llama.

f) Natural language processing (NLP):

Natural language processing of natuurlijke taalverwerking is een tak van AI die gebruikmaakt van machine learning, deep learning en linguïstiek om computers en verschillende andere apparaten in staat te stellen menselijke

tekst en spraak te detecteren, te herkennen, op te vangen en ermee te communiceren. NLP vereist enorme hoeveelheden gelabelde trainingsdata. NLP-technologie wordt veel gebruikt in zoekmachines, chatbots, virtuele assistenten, toepassingen voor grammaticacontrole, automatische vertaling en spraakgestuurde systemen. Bovendien helpen NLP-modellen bij het filteren van persoonsgegevens in grote hoeveelheden tekst, het identificeren van spam e-mails (bijvoorbeeld door slechte grammatica te identificeren), het samenvatten van lange tekstbestanden en het genereren van teksten die door mensen lijken te zijn geschreven.

Sommige factoren beïnvloeden de goede werking van de NLP-technologie. Dit zijn onder andere de bevooroordeelde trainingsdata, de lage kwaliteit of verwarrende invoer (bijv. gebruik van onjuiste grammatica, idioom en nieuw gecreëerde woorden, overmatige achtergrondruis, accenten). Zelfs in de communicatie van mens tot mens zit taal vol dubbelzinnigheden die niet in AI geprogrammeerd kunnen worden, of wel, maar niet zonder grote problemen. Daarom is het een grote uitdaging voor AI-programmeurs om deze problemen aan te pakken.

De meest voorkomende vormen van NLP in de praktijk zijn de volgende:

– Spraakherkenning (spraak-naar-tekst):

Spraakherkenning is het proces waarbij menselijke spraak wordt omgezet in geschreven tekstgegevens (de spraak is de invoer en de geschreven woorden zijn de uitvoer van het systeem). Deze technologie omvat linguïstiek, wiskunde en statistiek. Onder andere de volgende factoren kunnen de foutmarge van het systeem beïnvloeden: slechte uitspraak, accent, volume en achtergrondgeluid.

Spraakherkenning moet men niet verwarren met stemherkenning, dat erop gericht is de stem van een individu te identificeren.

Voorbeeld voor het notariaat: De notaris heeft de taak om een akte op te stellen die de notulen van een vergadering bevat. Hij/zij gebruikt een spraakherkennings-AI om de mondelinge uitspraken tijdens de vergadering om te zetten in tekstgegevens. Deze oplossing versnelt het notariële werk doordat de notaris geen lange pagina's meer hoeft te typen.

- **Natural language generation (NLG):** NLG is het omzetten van gestructureerde gegevens in een conversatie (geschreven of mondeling) in menselijke taal. Alexa van Amazon en Siri van Apple zijn twee alledaagse voorbeelden van deze technologie.

Voorbeeld voor het notariaat: De notaris wordt tijdens zijn/haar praktijk geconfronteerd met documenten die een specifieke taal gebruiken met termen die niet gemakkelijk te begrijpen zijn door juridische professionals (bijv. technische en bouwkundige documenten over onroerend goed, financiële overzichten, enz.) Om het eerste begrip van dergelijke inhoud te vergemakkelijken (en voordat een expert op dit gebied wordt geraadpleegd, indien nodig) wordt de NLG-oplossing toegepast om een eenvoudig te begrijpen samenvatting van het document te maken.

g) Computer vision:

Computer vision is een gebied van AI dat gebruik maakt van machine learning en neural networks om computers te leren betekenisvolle informatie te halen uit digitale afbeeldingen, video's en andere visuele input. Deze technologie werkt op dezelfde manier als menselijk zicht. Om computer vision te laten werken, hebben we voldoende rekenkracht nodig en een grote hoeveelheid trainingsdata die wordt analyseert totdat beelden worden herkend met de juiste nauwkeurigheid. Computer vision wordt tegenwoordig vooral gebruikt voor beeldclassificatie, objectdetectie in een afbeelding of video en vervolgens het volgen van objecten, evenals voor automatische beeldannotatie.

Een van de bekendste real-life toepassingen van de computer vision-technologie is de functie van Google Translate, waarmee mensen de camera van hun smartphone/tablet op een tekst in de ene taal kunnen richten en de vertaling in een andere taal krijgen. Bovendien maken zelfrijdende voertuigen hoofdzakelijk gebruik van computer vision-technologie.

h) Gezichtsherkenning:

Gezichtsherkenning is een AI-toepassing die een persoon identificeert of de identiteit van een persoon verifieert aan de hand van de kenmerken van zijn/haar gezicht in een afbeelding of video. Dit kan worden gedaan door te bepalen of gezichten in twee of meer afbeeldingen tot de-

zelfde persoon behoren of door het gezicht te vinden in een grote visuele dataset. Een van de meest wijdverspreide toepassingen van deze technologie is gezichtsherkenning door mobiele apparaten, maar het wordt ook gebruikt in andere beveiligingsoplossingen.

i) AI emotieherkenning en sentimentanalyse:

‘Een ‘emotieherkenningssysteem’ betekent een AI-systeem voor het identificeren of afleiden van emoties of intenties van natuurlijke personen op basis van hun biometrische gegevens’ [definitie AI Act, artikel 3, lid 39].

Gebaseerd op overweging 18 van de AI Act verwijst dit *‘begrip naar emoties of bedoelingen zoals geluk, verdriet, woede, verrassing, walging, verlegenheid, opwindend, schaamte, minachting, tevredenheid en vermaak. Lichamelijke toestanden zoals pijn of vermoeidheid vallen hier niet onder. Dit omvat ook niet de loutere detectie van duidelijk zichtbare uitingen, gebaren of bewegingen, tenzij deze worden gebruikt voor het identificeren of afleiden van emoties. Die uitdrukkingen kunnen eenvoudige gezichtsuitdrukkingen zijn, zoals een frons of een glimlach, of gebaren zoals de beweging van handen, armen of hoofd, of kenmerken van iemands stem, zoals een verheven stem of fluisteren.’*

AI emotieherkenning is een tak van AI die computers in staat stelt om non-verbale signalen zoals gezichtsuitdrukkingen, lichaamstaal, gebaren en stemtonen te analyseren om de emotionele toestand van natuurlijke personen te beoordelen (analyseren, interpreteren en classificeren). AI emotieherkenning gebruikt computer vision technologie en deep neural networks die betrekking hebben op de detectie van gezichtsemoties en de beoordeling van het sentiment op basis van visuele gegevens (afbeeldingen en video's) en ook op tekstanalyse (ook al valt dit laatste—omdat het geen biometrische gegevens zijn—niet onder de definitie van de AI Act).

De meeste trainingsdatabanken voor AI-emotieherkenning bestaan uit 2D statische beelden of 2D videosequenties; soms ook 3D-beelden. De emoties die een AI-model kan herkennen zijn afhankelijk van de getrainde klassen (bijv. boosheid, angst, blijdschap).

Voorbeeld voor het notariaat voor computer vision, gezichtsherkenning en sentimentanalyse: Een notaris heeft de taak om een authentieke akte op afstand op te stellen (d.w.z. een akte zonder de fysieke aanwezigheid van de cliënt, via videobellen, in een land waarvan het rechtssysteem dergelijke procedures toestaat). De notaris moet er onder andere voor zorgen dat de identiteit van de cliënt, de geschiktheid van zijn/haar omgeving voor de veiligheid van de videoconferentie en de vrije wil van de cliënt niet in het gedrang komen (hij/zij wordt bijvoorbeeld niet bedreigd). Met behulp van gezichtsherkenningstechnologie kan de notaris technische hulp krijgen om de identiteit van een cliënt te verifiëren. De AI vergelijkt het gezicht van de cliënt met de foto op het ID-document om er zeker van te zijn dat de persoon echt degene is die hij/zij beweert te zijn. Bovendien kan de technologie voor emotieherkenning en sentimentanalyse in hetzelfde proces op afstand de notaris helpen om te controleren of de cliënt niet onder druk staat, want als de aanwezigheid van druk wordt gedetecteerd, heeft de notaris de plicht om de taak niet af te ronden of om de cliënt te vragen persoonlijk naar het notariskantoor te komen. Daarnaast kunnen er ook andere computer vision-oplossingen worden gebruikt tijdens de procedure om de omgeving van de cliënt door de notaris te laten controleren om er zeker van te zijn dat er geen elementen aanwezig zijn die de legaliteit van de procedure in gevaar kunnen brengen. Terms related to the types and uses of AI systems

4. Begrippen met betrekking tot de soorten en het gebruik van AI-systemen

a) Parameters en gewichten:

Parameters bepalen hoe het model leert en uitvoert. De modelgrootte van het LLM is het aantal parameters: hoe meer parameters een model heeft, hoe complexer het is en hoe meer gegevens het kan verwerken. De parameters voor de LLM zijn afhankelijk van de specifieke taak waarvoor ze worden gebruikt. Voor complexe taken kan een model met een groot aantal parameters nodig zijn.

Gewichten (weights) zijn een subset van de parameters die de sterkte van verbanden tussen variabelen weergeven. Tijdens het trainingsproces kan de LLM de gewichten aanpassen om zijn prestaties te optimaliseren, d.w.z.

om de fout tussen de voorspelde uitvoer en de werkelijke uitvoer te minimaliseren.

b) Prompts:

Prompts zijn invoervragen van de gebruikers van generatieve AI-systemen. Deze systemen genereren specifieke outputs op basis van de prompts.

Generatieve AI vertrouwt op de herhaalde verfijning van verschillende aanwijzingen om effectief te leren van invoergegevens en nauwkeurigere antwoorden (output) te produceren. De rol van het zogenaamde prompt engineering is het maken en verfijnen van queries die helpen om generatieve AI-modellen de nuances van de gegeven query te laten begrijpen, waardoor de kwaliteit van de door AI gegenereerde inhoud wordt verbeterd.

Voorbeeld voor het notariaat: De notaris wil een AI-oplossing gebruiken om de clausules uit een koop- en verkoopcontract te halen die betrekking hebben op verplichtingen van de verkoper. Om ze te krijgen, is een van de mogelijke formuleringen van de prompt die de notaris in het systeem moet typen of spreken: 'Haal de clausules over de verplichtingen van de verkoper eruit.' Hoe nauwkeuriger de prompt is geformuleerd, hoe beter en nauwkeuriger de kwaliteit van de output.

5. Belangrijkste deelnemers aan het AI-ecosysteem

a) Provider:

"Aanbieder": een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of ander orgaan dat een AI-systeem of een AI-model voor algemeen gebruik ontwikkelt of dat een AI-systeem of een AI-model voor algemene doeleinden heeft ontwikkeld en op de markt brengt of het AI-systeem onder zijn eigen naam of handelsmerk in gebruik neemt, al dan niet tegen betaling. [definitie AI Act, Artikel 3, lid 3]

Voorbeeld voor het notariaat: De aanbieder van notariële AI-systemen kan bijvoorbeeld de notariële organisatie zijn waar de individuele notaris lid van is (internationaal ontwikkeld AI-systeem) of een andere externe entiteit (extern ontwikkeld AI-systeem) die dergelijke systemen ontwikkelt voor gebruik door notarissen.

b) Deployer (gebruiker):

‘Gebruiker: een natuurlijke of rechtspersoon, overheidsinstantie, agentschap of andere instantie die gebruik maakt van een AI-systeem onder zijn gezag, behalve wanneer het AI-systeem wordt gebruikt in het kader van een persoonlijke, niet-beroepsmatige activiteit [definitie AI Act, artikel 3, lid 4]

Voorbeeld voor het notariaat: De gebruikers van AI-systemen kunnen de notariële organisaties of de individuele notarissen zelf zijn.

6. Kwesties en verschijnselen met betrekking tot AI

a) AI-hallucinatie:

AI-hallucinatie is een fenomeen waarbij LLM's—meestal generatieve AI-modellen—niet-bestaande patronen of objecten waarnemen en onnauwkeurige output creëren, die vaak volledig realistisch lijkt en die in staat is de gebruiker te misleiden.

Belangrijk om op te merken is dat AI-hallucinatie niet gelijk is aan menselijke hallucinatie; de term wordt alleen gebruikt om dit fenomeen te beschrijven.

Er zijn verschillende manieren bekend om AI-hallucinatie aan te pakken, zoals het gebruik van hoogwaardige trainingsdata, het vaststellen van het exacte doel van het AI-systeem, het beperken van de output, het continu testen van het model en—als allerbelangrijkste—het uitoefenen van menselijk toezicht op en validatie van de output.

Voorbeeld voor het notariaat: Een notaris wil toegang tot de jurisprudentie met betrekking tot crypto-transacties. Het systeem somt en beschrijft gevallen op die nooit hebben bestaan en geen basis hebben. Door deze valse output te geven, wordt de indruk gewekt dat zulke gevallen echt zijn. Door de suggesties van de AI te controleren, identificeert de notaris de zaken die door het AI-systeem zijn verzonnen.

b) Black box AI:

Black box AI betekent dat het moeilijk of onmogelijk is om het AI-besluitvormingsproces te begrijpen. Vaak zijn zelfs de ingenieurs of datawetenschappers die het toege-

paste algoritme ontwikkelen niet in staat om te begrijpen of uit te leggen wat er achter de schermen gebeurt en hoe het tot een specifieke output komt. Dit heeft een negatief effect op de transparantie van de werking van het AI-model en op de verklaarbaarheid van de output. Het black box-fenomeen is het meest typisch bij—maar niet beperkt tot—generatieve AI-modellen.

Voorbeeld voor het notariaat: De notaris gebruikt een AI-oplossing die aanbevelingen geeft voor een complexe juridische kwestie. De notaris zelf wil graag begrijpen waarom het systeem de gegeven output heeft geleverd, maar kan noch de redenen achter de besluitvorming van de AI, noch het proces zelf begrijpen. Dat geldt ook voor de AI-ontwikkelaar zelf; die kan daarin dus ook geen hulp bieden. Vanwege het gebrek aan verklaarbaarheid besluit de notaris de AI-aanbevelingen terzijde te schuiven.

c) AI-bias:

AI-bias betekent het optreden van bevooroordeelde outputs door AI-systemen als gevolg van de eigenschappen van het menselijk brein (mensen zijn van nature bevooroordeeld en AI-systemen worden ontwikkeld door mensen) die in AI verschijnen, meestal door de vooringenomen trainingsdata en de vooroordelen die—vaak onbewust—door de programmeurs in het algoritme zijn opgenomen. Het AI-systeem zal waarschijnlijk vooroordelen repliceren in de output, wat leidt tot onnauwkeurig functioneren. Vroegtijdige en continue bewaking, detectie en beperking van bias is cruciaal voor de betrouwbaarheid van de AI-systemen.

Voorbeeld voor het notariaat: Het AI-systeem gebruikt door de notaris was voornamelijk getraind op transacties met een hoog witwasrisico van cliënten uit een bepaald land. Het AI-systeem kan op basis hiervan een vooroordeel ontwikkelen voor andere personen uit datzelfde land, zelfs als hun voorgenomen transacties geen risico op witwassen inhouden, waardoor hun transacties door het systeem als verdacht worden gemarkeerd.

d) Overfitting en underfitting:

Overfitting treedt op wanneer het AI-model de trainingsdata ‘te goed’ leert, waardoor het moeilijk generaliseert naar nieuwe data. Underfitting gebeurt als het AI-model er niet in slaagt de onderliggende patronen in de data te

identificeren, wat resulteert in zwakke prestaties op de testdatasets. Beide hebben het risico van onbetrouwbare en onnauwkeurige output en moeten daarom worden beperkt bij het evalueren van de prestaties van het AI-model.

Voorbeeld voor het notariaat: Als het AI-systeem van de notaris te veel is getraind op specifieke contracten (bijv. koop en verkoop), kan het leren patronen te herkennen die alleen van toepassing zijn op die contracten en kan het niet correct te werk gaan bij andere contracten (bijv. schenkingen), wat resulteert in onjuiste output (overfitting). Aan de andere kant, als het AI-systeem niet voldoende getraind is voor een bepaald type contracten, kan het patronen die in contracten van dat type moeten worden gebruikt niet herkennen (underfitting).

e) AI-feedbackloop:

Een AI-feedbackloop is een proces waarbij een AI-systeem feedback ontvangt van verschillende bronnen (mensen, andere systemen, etc.) over zijn functioneren en deze feedback gebruikt om zijn algoritme en prestaties te verbeteren. Dit proces wordt later in verschillende fasen herhaald, waardoor het AI-systeem voortdurend kan leren. De feedbackloop kan een probleem vormen wanneer de invoergegevens niet de juiste hoeveelheid of kwaliteit hebben, de feedback vertekend is of de toegepaste technologie niet toereikend is.

Het opnemen van menselijke feedback in de feedbackloop kan de prestaties van een AI-systeem optimaliseren door gebieden te identificeren waar verbetering nodig is. Als een chatbot bijvoorbeeld niet goed reageert op bepaalde soorten vragen, kan menselijke feedback helpen deze problemen te identificeren.

Voorbeeld voor het notariaat: De notaris gebruikt een AI-systeem waarvan de output in bepaalde opzichten (bijv. het aanbevelen van ongeschikte clausules in het gegeven contract) voortdurend door hem/haar wordt afgeslagen. Op basis van deze feedback van menselijke experts kan het systeem zijn werking aanpassen door het aantal dezelfde of soortgelijke outputs te verminderen.

f) Human-in-the-loop (HITL):

Human-in-the-loop is een gezamenlijke aanpak waarbij menselijke input wordt geïntegreerd in machine learning

en AI-systemen door mensen die actief deelnemen aan de training, evaluatie en werking van ML-modellen. HITL is gericht op het verbeteren van de nauwkeurigheid, betrouwbaarheid en aanpasbaarheid van ML-modellen en helpt bij het verminderen van bias.

Bovendien helpen de inzichten van mensen om beslissingen van modellen te verklaren. De menselijke input varieert van het labelen van trainingsdata en het evalueren van de prestaties van het AI-model tot het geven van feedback op zijn acties. De menselijke betrokkenheid vergroot het aanpassingsvermogen van AI en zorgt ervoor dat AI-modellen evolueren aan de hand van gebruikersvoorkeuren en scenario's uit de echte wereld.

Voorbeeld voor het notariaat: De notaris gebruikt een AI-oplossing voor het geautomatiseerd opstellen van documenten. Bij het controleren van de output van het systeem detecteert hij/zij verschillende onnauwkeurigheden en anomalieën. Daarom gooit hij/zij (delen van) de output weg en voegt hij/zij zelfgeschreven clausules toe. Om de ontwikkelaar bewust te maken van deze tekortkomingen, informeert de notaris de ontwikkelaar hierover en doet hij/zij voorstellen om het systeem te verbeteren.

g) Automation bias:

Met automation bias wordt de neiging van mensen bedoeld om te veel te vertrouwen op suggesties van geautomatiseerde besluitvormingssystemen en om tegenstrijdige informatie te negeren die zonder automatisering is gemaakt, zelfs als deze correct is.

Voorbeeld voor het notariaat: Een medewerker van de notaris begint te veel te vertrouwen op de output van het AI-systeem voor het beoordelen van documenten en accepteert elke wijziging die door het systeem wordt voorgesteld zonder de nauwkeurigheid ervan te controleren. Dit brengt het grote risico met zich mee dat de niet-geverifieerde notariële akten onjuiste clausules en onnauwkeurigheden bevatten, met negatieve juridische gevolgen.

h) Deepfake:

'Deepfake betekent door AI gegenereerde of gemanipuleerde beeld-, geluids- of video-inhoud die lijkt op bestaande personen, voorwerpen, plaatsen, entiteiten of gebeur-

tenissen en die voor een persoon valselyk authentiek of waarheidsgetrouw lijkt'. [definitie AI Act, artikel 3, lid 60]

Deepfakes worden vaak met kwade bedoelingen gegenereerd en gebruikt om verkeerde informatie te verspreiden of cybercriminaliteit te plegen.

Voorbeeld voor het notariaat: Bij een notariële procedure op afstand vermoedt de notaris dat de gezichtsopname van de cliënt die hij/zij op het scherm ziet niet echt is, maar een deepfake. Met behulp van gezichtsherkennings-AI kan de notaris er zeker van zijn dat dit het geval is en weigeren verder te gaan.

7. Belangrijkste juridische bronnen met betrekking tot AI

a) Artificial Intelligence Act (AI Act):

Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828

De AI Act is wereldwijd de eerste alomvattende wettelijke regeling inzake AI die in de EU van toepassing is met een extraterritoriale werking en die geleidelijk in werking treedt. De AI Act volgt een risicogebaseerde aanpak waarbij AI kan worden onderverdeeld in 4 risicocategorieën (verboden AI-praktijken, AI-systemen met een hoog risico, bepaalde AI-systemen met transparantieplichtingen en een minimaal risico) die verschillende verplichtingen met zich meebrengen voor de deelnemers van het AI-ecosysteem (meestal aanbieders en gebruikers). Bij het ontwikkelen en/of gebruiken van AI-systemen moeten notariële organisaties en notarissen de bepalingen van de AI Act strikt naleven. Dit handboek beoogt de mogelijke gevallen in kaart te brengen waarin de regels van de AI Act in de notariële context moeten of kunnen worden toegepast.

b) Kaderverdrag van de Raad van Europa inzake Kunstmatige Intelligentie en Mensenrechten, Democratie en de Rechtsstaat:

Dit is het eerste internationale wettelijk bindende verdrag dat respect voor de mensenrechten, de rechtsstaat

en de democratie bij het gebruik van AI-systemen moet waarborgen. Het Verdrag is van toepassing op de gehele levenscyclus van AI-systemen en pakt hun belangrijkste risico's aan (hanteert een risicogebaseerde aanpak). Het omvat het gebruik van AI-systemen in de publieke en private sector. In het document zijn vereisten voor transparanties en toezicht opgesteld en het vereist dat de partijen oplossingen implementeren om mogelijke risico's te identificeren, te voorkomen en/of te beperken. Bovendien staan het respect voor gelijkheid, het verbod op discriminatie en het recht op privacy ook centraal in het verdrag.

c) DSM Copyright Directive:

Richtlijn (EU) 2019/790 van het Europees Parlement en de Raad van 17 april 2019 inzake auteursrechten en naburige rechten in de digitale eengemaakte markt en tot wijziging van Richtlijnen 96/9/EG en 2001/29/EG

De DSM Copyright Directive introduceerde de zogenaamde tekst- en datamining uitzonderingen en beperkingen die cruciaal zijn voor de efficiënte training van de AI-modellen. De relevante regels dragen bij aan de legaliteit van het trainingsproces door inbreuken op het auteursrecht, naburige rechten en databankrechten te vermijden wanneer het AI-model wordt getraind met beschermde werken.

d) Algemene Verordening Gegevensbescherming (AVG):

Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 5/46/EG

AI—met name generatieve AI-modellen—kan leiden tot ernstige zorgen met betrekking tot de bescherming van de privacy en persoonsgegevens. Daarom moet er serieus rekening gehouden worden met de AVG en de relevante regels van de AI Act. In dit handboek is een apart hoofdstuk gewijd aan het effectief voorkomen van mogelijke inbreuken op persoonsgegevens tijdens de ontwikkeling en het gebruik van AI-systemen.

III. Mogelijke manieren van AI-gebruik door notarissen

1. Algemene inzichten

Ondanks de risico's die verbonden zijn aan het gebruik van AI-oplossingen—mits op de juiste manier gebruikt—biedt deze technologie kansen en voordelen voor het notariaat. In de eerste plaats moet worden benadrukt dat technologie in het algemeen—inclusief AI—geen doel op zich kan zijn, maar een hulpmiddel voor de beroepsgroep om diensten van hogere kwaliteit te leveren en het werk van notarissen te vergemakkelijken.

Bij het bepalen van de mogelijke manieren van gebruik van AI door notarissen is het belangrijk rekening te houden met het feit dat, hoewel alle bij de CNUE aangesloten notariaten behoren tot de groep van notarissen van het Latijnse type, er aanzienlijke verschillen kunnen zijn tussen de 22 CNUE-leden, voornamelijk met betrekking tot hun status (sommige notariaten zijn bijvoorbeeld nauwer verbonden met het rechtssysteem—d.w.z. de status van rechtbanken en rechters—dan andere) en hun competenties. Deze kenmerken kunnen ertoe leiden dat sommige notariaten anders gebruik kunnen maken van bepaalde AI-oplossingen dan andere. In dit handboek proberen we de meest voorkomende mogelijke manieren van AI-gebruik in de 22 bij de CNUE aangesloten notariaten te identificeren en te presenteren.

Hieronder worden de meest plausibele AI-toepassingen door notarissen—niet uitputtend—gepresenteerd, zonder in te gaan op de bijbehorende risico's. Die risico's—inclusief de verboden AI-praktijken en de AI-systemen met een hoog risico—worden afzonderlijk besproken in de volgende hoofdstukken. Het is belangrijk om te benadrukken dat notarieel gebruik van AI alleen kan worden uitgevoerd als de wetgever toestemming geeft of als het niet verboden is.

2. Algemene voordelen van het gebruik van AI

Zoals wordt vermeld in talrijke wetenschappelijke bronnen over dit onderwerp, dragen AI-oplossingen ook bij aan de automatisering van bepaalde taken op het gebied van recht. Deze hebben meestal betrekking op routinetaken die gerelateerd kunnen worden aan het juridische werk

(bijv. het opstellen van notulen met behulp van de spraak-naar-tekst toepassingen) of aan de administratie van het notariaat (bijv. afhandelen van verzoeken om afspraken van cliënten, facturering). Deze oplossingen dragen bij aan het stroomlijnen van professionele workflows en het verhogen van de werkefficiëntie en productiviteit, waar uiteindelijk de cliënten van de notarissen van profiteren.

De menselijke inzet (notarissen en notariële medewerkers) die op deze manier wordt gespaard, kan worden gebruikt voor diepgaandere en complexe juridische taken die de mate van creativiteit vereisen die AI-systemen momenteel niet hebben. Bovendien kunnen de toegepaste AI-oplossingen op de middellange en lange termijn leiden tot aanzienlijke kostenbesparingen voor de notariskantoren. Bovendien biedt het gebruik van AI-systemen de mogelijkheid om meer gegevens te onderzoeken en te verwerken, niet alleen door notarissen maar ook door notariële organisaties.

Zoals later zal worden behandeld, kan het notariële kernwerk, dat uitgebreide juridische kennis en ervaring vereist—vanwege de inherente tekortkomingen van de huidige AI-systemen—niet vervangen worden door AI.

3. Specifieke manieren van AI-gebruik door het notariaat

a) Documentautomatisering

Documentautomatisering, d.w.z. het maken van notariële akten met behulp van AI, met behulp van technologieën zoals NLP en LLM's, kan belangrijke voordelen hebben voor het beroep. Dit kan het geval zijn voor het genereren van eenvoudige routinedocumenten (bijv. attesten, certificaten) of het creëren van akten op basis van sjablonen (bijv. de Europese erfrechtcertificaten). Daarnaast is het automatiseren van sommige 'post-contractuele' formele taken (bijvoorbeeld voor het uitvoeren van akten) ook mogelijk met behulp van AI-oplossingen. Er moet worden benadrukt dat automatisering van documenten in geen geval betekent dat notarissen worden uitgesloten van het proces van het opstellen van de relevante akten. Zelfs in het geval van een automatisch gegenereerde akte heeft de

notaris de verplichting om deze nauwkeurig te reviseren en de eventuele fouten van het systeem te corrigeren. Daarom moeten AI-toepassingen voor documentautomatisering alleen dienen als hulpmiddelen voor notarissen, vooral om tijd te besparen op het helemaal opnieuw opstellen van documenten.

b) Documenten beoordelen

Aan het einde van het opstellen van notariële akten kunnen LLM's voor het nakijken van documenten efficiënt worden gebruikt als aanvulling (geen vervanging) voor het controleren van de volledigheid van de gegeven handeling, het controleren van ontbrekende clausules die relevant zijn voor de context en het identificeren van mogelijk conflicterende clausules en termen. Dit kan ook inhouden dat de consistentie van de notariële akte met eerdere akten met betrekking tot dezelfde/gelijksoortige goederen en/of personen wordt gecontroleerd. Bovendien kan AI worden gebruikt om te controleren of de wet overeenstemt met de laatste wetswijzigingen. Deze verbeteren de nauwkeurigheid van notariële diensten en helpen menselijke fouten te beperken.

c) Spraak-naar-tekst transcripties

In gevallen waarin notarissen notulen en soortgelijke documenten moeten opstellen, kunnen NLP tools de procedure versnellen en stroomlijnen door het toepassen van spraak-naar-tekst technologie, uiteraard met de daaropvolgende controle van de tekst door de notaris.

d) Samenvatten van documenten en hulp bij analyse

Vaak moeten notarissen talloze documenten met een groot aantal pagina's identificeren en analyseren, variërend van officiële rechtshandelingen tot documenten die nodig zijn voor hun notariële akten en procedures. NLP en LLM oplossingen kunnen ook helpen bij het vinden en samenvatten van dergelijke documenten, het extraheren van de relevante clausules, artikelen en paragrafen en het benadrukken van de belangrijkste wijzigingen ten opzichte van eerdere versies van dergelijke teksten. Dit ontslaat de notaris echter niet van zijn/haar plicht om de documenten persoonlijk door te nemen, aangezien niet kan worden gegarandeerd dat de AI geen belangrijke informatie weglaat.

e) Gezichtsherkenning, emotieherkenning en sentimentanalyse

In de afgelopen jaren zijn notariële akten op afstand een realiteit geworden die nu veel voorkomt in de praktijk van verschillende notariaten van de CNUE. Dit is met name het geval voor notariaten met uitgebreide competenties op het gebied van de oprichting van vennootschappen, waar de relevante EU-regels het verplicht maakten om notariële diensten op afstand te introduceren (d.w.z. het opstellen van de relevante notariële akten zonder de fysieke aanwezigheid van de cliënt bij de notaris, door gebruik te maken van videobellen).

In deze processen is de veilige en efficiënte verificatie van de identiteit van de klant een cruciale stap, waarvoor AI-tools voor biometrische gezichtsherkenning hulp kunnen bieden. Deze hulpmiddelen dienen als aanvulling op de menselijke identificatie van de cliënt door de notaris, waardoor ze bijdragen aan de rechtszekerheid en aan de verspreiding van notariële diensten op afstand. Om de veiligheid van dergelijke procedures te vergroten kunnen emotieherkenning en sentimentanalyse ook worden ingezet om te detecteren of de betreffende cliënt onder druk of dwang staat. Deze oplossingen zijn in staat om nuances te detecteren in de bewegingen, gebaren en andere fysieke en psychologische kenmerken van natuurlijke personen, die niet of moeilijker door het menselijk oog kunnen worden gedetecteerd. Bij het toepassen van dergelijke oplossingen moet de notaris er rekening mee houden dat AI alleen assistentie biedt en dat hij/zij verplicht is om de output van de machine niet automatisch te accepteren (onder andere vanwege automation bias).

Verder moet worden benadrukt dat systemen voor emotieherkenning—als ze niet onder de verboden praktijken van de AI Act vallen—worden beschouwd als 'hoog risico systemen' overeenkomstig punt 1, onder c), van bijlage III bij de AI Act met bijzondere transparantieverplichtingen krachtens dezelfde AI Act [Artikel 50, lid 3].

f) Opslag, classificatie en terugvinden van documenten

Nu al kunnen eenvoudigere ML tools helpen bij het beheer van notariële akten na het opstellen, door de notarissen te helpen bij het opslaan, classificeren en snel

terugvinden van documenten. Dit kan bijdragen aan een effectief beheer van de dossiers van cliënten.

g) Automatisch toezicht op wetwijzigingen en nieuwe jurisprudentie

In het dagelijkse werk, maar ook in de opleiding van notarissen, kunnen AI-systemen uiterst nuttig zijn door permanent toezicht te houden op de veranderingen in de wetgeving en de nieuwe jurisprudentie die van invloed zijn op de notariële activiteiten, waardoor men snel toegang heeft tot relevante juridische informatie. Bovendien kunnen bij het gebruik van sjablonen voor bepaalde notariële activiteiten de relevante wijzigingen automatisch in die sjablonen worden opgenomen.

h) Machinevertaling

AI-gebaseerde automatische vertaaltools zijn wijdverspreid in de professionele wereld, en de notarissen zijn daar geen uitzondering op. Tools die ook gratis of tegen een lage prijs beschikbaar zijn (bijv. DeepL translate) kunnen effectief worden gebruikt om de communicatie met klanten in vreemde talen te versnellen en ook—met strikte beperkingen—voor de voorbereiding van notariële handelingen. Machinevertaling kan echter niet in de plaats komen van voldoende kennis van de gegeven taal bij de notaris. Daarom moet, indien de notaris (of een van zijn/haar werknemers) onvoldoende kennis heeft van de taal van de communicatie/van de handeling, het gebruik van machinevertaling worden vermeden, aangezien de menselijke controle van de vertaalde output niet veilig kan worden uitgevoerd.

i) Notariële chatbots

Met betrekking tot de communicatieactiviteiten van het notariaat kunnen chatbots nuttige hulpmiddelen zijn. Deze kunnen variëren van eenvoudigere regelgebaseerde chatbots tot meer geavanceerde AI-chatbots. Aangezien AI niet in staat is om gepersonaliseerde juridische diensten te verlenen aan cliënten, moet de rol van deze chatbots beperkt blijven tot het verstrekken van zeer algemene informatie over de meest gestelde juridische vragen op notarieel gebied. Deze beperking moet in elk geval worden aangegeven aan de cliënten. Gepersonaliseerde juridische diensten zouden alleen moeten worden aangeboden door notarissen (mogelijk met AI-ondersteuning), aangezien chatbots en AI-systemen niet in staat zijn om de omstan-

digheden en de context te herkennen waarin de juridische oplossingen nodig zijn.

In het geval van complexere AI-chatbots kunnen de door gebruikers ingevoerde gegevens bovendien worden gebruikt om het systeem verder te ontwikkelen en ook om informatie te krijgen over de meest gestelde vragen, zodat de concurrerende notariële organisaties statistieken kunnen krijgen over de meest geraadpleegde gebieden en de notariële diensten op deze gebieden kunnen stroomlijnen.

j) AI voor de beveiliging van gegevens en notariële systemen

AI-oplossingen kunnen effectief worden gebruikt om bij te dragen aan de beveiliging van notariële gegevens en systemen en om cyberaanvallen te voorkomen ('cyberveiligheid met AI').

4. Implementatie van AI-oplossingen door het notariaat

Afhankelijk van de beslissing van de bevoegde notariële organisatie of notaris kunnen de bovenstaande oplossingen worden ingevoerd als modules of integrale onderdelen van multifunctionele managementsoftware of worden gebruikt als op zichzelf staande oplossingen voor de verschillende taken. De eerste heeft het voordeel dat verschillende oplossingen onder één dak worden samengebracht en een consistenter en beter geïntegreerd systeem bieden, de tweede heeft het voordeel dat het gemakkelijker onafhankelijk te verbeteren is door zich alleen op het doel te richten.

Belangrijkste conclusies

- AI-technologie is een hulpmiddel voor het notariaat om diensten van hogere kwaliteit te leveren en het werk van notarissen makkelijker te maken.
- AI-systemen dragen vooral bij aan de automatisering van notariële routinetaken.
- De kern van het notariële werk (dat uitgebreide juridische kennis en ervaring vereist) kan en mag niet worden vervangen door AI.
- Documentautomatisering (d.w.z. het maken van notariële akten met behulp van AI) is een van de toepassingsgebieden van de technologie in het notariaat, met name voor het maken van eenvoudige routinedocumenten en akten op basis van sjablonen.
- Technologieën voor gezichtsherkenning, emotieherkenning en sentimentanalyse kunnen de notaris helpen bij het op afstand (d.w.z. via videobellen) verifiëren van de identiteit van de cliënt en de vrije en vrijwillige uitdrukking van zijn/haar wil.
- Bepaalde AI-tools kunnen worden gebruikt om de volledigheid en correctheid van notariële akten te reviseren en om te helpen bij het opslaan, classificeren en gemakkelijk terugvinden van dergelijke akten.
- Machinevertaling wordt alleen aanbevolen als de notaris de betreffende talen op voldoende niveau spreekt.
- De notaris moet de output van AI-systemen controleren en zo nodig aanpassen alvorens deze te accepteren.
- De verschillende AI-oplossingen kunnen worden ingezet als onderdeel van de notariële managementsoftware of worden gebruikt als zelfstandige toepassingen voor de verschillende taken.

IV. Toepasselijkheid van de EU Artificial Intelligence Act

1. Algemene inzichten en tijdlijn

Op 12 juli 2024 wordt de Artificial Intelligence Act (AI Act) van de Europese Unie gepubliceerd in het Publicatieblad van de Europese Unie en trad 20 dagen later, op 1 augustus, in werking. De AI Act is een rechtstreeks toepasselijke EU-regelgeving en is wereldwijd de eerste uitgebreide reeks wettelijke regels inzake AI met een zogenaamde risicogebaseerde aanpak. De verplichtingen uit de AI Act worden geleidelijk van toepassing. Het doel van de AI Act is om AI-innovatie binnen de EU te bevorderen en de grondrechten van burgers en de rechtsstaat te beschermen.

Voor de duidelijkheid worden in dit hoofdstuk alleen de regels van de AI Act behandeld die van toepassing kunnen zijn op het notariaat. Men moet zich er echter van bewust zijn dat de AI Act talrijke bepalingen bevat die verschillende AI-systemen reguleren. Deze bepalingen worden hier niet geanalyseerd omdat ze niet kunnen worden gebruikt voor notariële activiteiten.

De gefaseerde invoering betekent dat als hoofdregel de AI Act binnen 24 maanden na inwerkingtreding, d.w.z. vanaf 2 augustus 2026, volledig van toepassing zal zijn. De bepalingen over het verbod op verboden praktijken zijn van toepassing vanaf 6 maanden na de inwerkingtreding, d.w.z. vanaf 2 februari 2025. Bovendien heeft de wetgever een termijn van 12 maanden vastgesteld voor de toepassing van governanceregels en -verplichtingen voor General Purpose AI (GPAI) modellen (2 augustus 2025).

2. Persoonlijke en territoriale reikwijdte

De AI Act heeft een brede persoonlijke reikwijdte die de volgende categorieën omvat:

- Aanbieders;
- Gebruikers;
- Importeurs; en
- Distributeurs van AI-systemen

Vanuit het perspectief van het notariaat zijn alleen de categorieën van ‘aanbieder’ en ‘gebruiker’ relevant. Volgens de definitie van de AI Act is de aanbieder een natuurlijke

of rechtspersoon overheidsinstantie, agentschap of ander orgaan dat een AI-systeem of een general-purpose AI model ontwikkelt of laat ontwikkelen en op de markt brengt of het AI-systeem onder eigen naam of handelsmerk, al dan niet tegen betaling, in gebruik neemt [artikel 3, lid 3]. De AI Act bevat geen beperking ten aanzien van het beroep en de status van de aanbieder. Als een notariële organisatie dus een AI-systeem ontwikkelt, wordt het geclassificeerd als een aanbieder van het gegeven systeem.

De rol van de gebruiker wordt door de AI Act toegekend aan natuurlijke of rechtspersonen, overheidsinstanties, agentschappen of andere partijen die gebruik maken van een AI-systeem onder hun gezag, tenzij het AI-systeem wordt gebruikt in het kader van een persoonlijke, niet-beroepsmatige activiteit [artikel 3, lid 4]. Als notarissen dus AI-systemen voor notariële activiteiten gebruiken, vallen ze onder de categorie van ‘gebruiker’. Deze bepaling betekent echter niet dat notarissen altijd onderworpen zijn aan de AI Act, aangezien bijvoorbeeld het gebruik van een AI-systeem buiten hun professionele activiteiten (bijv. ChatGPT voor het schrijven van privé e-mails) niet valt onder het toepassingsgebied van de EU Verordening.

Benadrukt moet worden dat de definities van ‘aanbieder’ en van ‘gebruiker’ uitdrukkelijk betrekking hebben op overheidsinstanties, en met betrekking tot bepaalde artikelen (bv. de verplichting van een beoordeling van de gevolgen voor de grondrechten) is deze status van bijzonder belang. Als dus in een EU-lidstaat een individuele notaris of een notariële organisatie die het notariaat van die lidstaat vertegenwoordigt, door de nationale wetgeving wordt beschouwd als een overheidsinstantie, kunnen de relevante specifieke regels van toepassing zijn.

Moeilijkheden om te bepalen of een natuurlijke of rechtspersoon in aanmerking komt als een aanbieder of een gebruiker kunnen zich met name voordoen wanneer hij/zij niet alleen gebruik maakt van een bestaand AI-systeem maar een aanzienlijke wijziging aanbrengt in een systeem dat al op de markt is gebracht of al in gebruik is genomen. In dit geval wordt de opgegeven natuurlijke- of rechtspersoon beschouwd als aanbieder van het systeem op voorwaarde dat het systeem werd gekwalificeerd als hoog risico en ook na de wijziging in die categorie blijft.

Hetzelfde kan gebeuren als de gebruiker het beoogde doel van een AI-systeem zonder hoog risico zodanig aanpast dat het een AI-systeem met een hoog risico wordt [Artikel 25, lid 1, onder b) en c)].

Benadrukt moet worden dat de kwalificatie van een notariële organisatie en/of een notaris als een ‘aanbieder’ of ‘gebruiker’ niet automatisch betekent dat verdere bepalingen van de AI Act ook op hen van toepassing zijn. Tegelijkertijd—op voorwaarde dat aan bepaalde criteria wordt voldaan—bepaalt hun indeling in een van deze categorieën aan welke verplichtingen ze moeten voldoen, en dit is te wijten aan het feit dat er verschillende verplichtingen gelden voor ‘aanbieders’ en ‘gebruikers’.

Net als de Algemene Verordening Gegevensbescherming (AVG) heeft de AI Act ook een brede extraterritoriale reikwijdte (d.w.z. is ook van toepassing op aanbieders en gebruikers die buiten het grondgebied van de EU zijn gevestigd in vooraf bepaalde gevallen). In het geval van het notariaat zijn echter zowel de notariële organen als de individuele notarissen altijd op het grondgebied van de EU gevestigd, en daarom is het territoriale toepassingsgebied van de AI Act altijd op hen van toepassing (bij kwalificatie als ‘aanbieders’ of ‘gebruikers’ en als aan verdere criteria wordt voldaan voor de toepassing van de AI Act).

3. Het risicocategorisatiesysteem

Op basis van de regels van de AI Act kunnen we AI-systemen indelen in 4 risicocategorieën. De eerste categorie omvat AI-systemen waarvan gebruik verboden is door de AI Act omdat ze een onaanvaardbaar risico vormen voor de grondrechten van burgers. Binnen de EU kunnen dergelijke AI-systemen niet worden geleverd of gebruikt. Zoals eerder vermeld is het verbieden van deze systemen zo cruciaal voor de wetgever, dat dit de eerste systemen zijn die verboden worden onder de AI Act. Dit verbod geldt vanaf 6 maanden na de inwerkingtreding van de AI Act (vanaf 2 februari 2025).

De tweede categorie, AI-systemen met een hoog risico, is de belangrijkste focus van de AI Act. Zowel de aanbieders als de gebruikers van dergelijke systemen moeten voldoen aan strenge en uitgebreide verplichtingen die worden voorgeschreven door de AI Act (zie hieronder).

De derde categorie wordt door de AI Act gedefinieerd als ‘bepaalde AI-systemen met transparantieplichtingen’,

wat aangeeft dat de aanbieders en gebruikers van dergelijke systemen meestal (maar niet altijd) zijn onderworpen aan transparantieplichtingen.

Tot slot, zelfs als een dergelijke categorie niet expliciet wordt genoemd in de AI Act, worden AI-systemen met een minimaal risico in de praktijk gezien als de vierde categorie.

Deze systemen vallen niet onder het materiële toepassingsgebied van de AI Act. Verschillende auteurs en professionals erkennen ook het bestaan van de categorie ‘risicoloze’ AI-systemen. Bij AI is er echter altijd een soort risico aanwezig, ook al is dat zeer minimaal, los van de regels van de AI Act.

4. Categorisering van (potentiële) notariële AI-oplossingen onder de AI Act

Bij dit onderdeel wordt bepaald onder welke categorieën AI-systemen (mogelijk) door het notariaat ontwikkeld/ingezet kunnen worden. De identificatie van de categorieën is een weerspiegeling van de huidige interpretatie van de AI Act. Het is gebaseerd op de belangrijkste notariële activiteiten in heel Europa en is niet sluitend. Dit betekent dat er in verschillende landen notariële AI-gebruiksgevallen kunnen zijn die niet in dit Handboek worden beschreven, maar die wel onder een van de categorieën kunnen vallen die in de AI Act staan. Daarom moet er altijd een grondige analyse plaatsvinden van het gebruik van AI voor de afzonderlijke notariële activiteiten. Tot slot, afhankelijk van verdere interpretatie en verduidelijking—inclusief door het Hof van Justitie van de Europese Unie—kan de categorisering veranderen.

a) Verboden praktijken

De AI Act bevat een volledige opsomming van de verboden AI-praktijken. Inherent aan de notariële activiteiten is de bescherming van de grondrechten van burgers. Aangezien de verboden praktijken onder andere betrekking hebben op systemen die individuen manipuleren, hun kwetsbaarheden misbruiken, hun gevoelige persoonsgegevens verzamelen zonder toestemming of sociale scores maken door scores toe te kennen op basis van menselijk gedrag, die de toegang tot diensten of andere mogelijkheden beïnvloeden, enzovoort, is het duidelijk dat geen enkele nota-

riële activiteit het gebruik van een AI-systeem vereist dat onder deze categorie kan vallen.

Echter, voor hun veiligheid moeten notarissen en notariële organisaties bij het ontwikkelen of gebruiken van een AI-systeem altijd controleren of het betreffende AI-systeem onder deze categorie valt. De AI Act [artikel 5, lid 1, onder f)] verbiedt het op de markt brengen, aanbieden of gebruik van AI-systemen om emoties van een natuurlijke persoon af te leiden op het gebied van werk, behalve wanneer het gebruik van het AI-systeem bedoeld is om te worden ingevoerd of op de markt gebracht om medische of veiligheidsredenen. Deze bepaling verbiedt de emotieherkennungssystemen die emoties van natuurlijke personen identificeren of afleiden op basis van biometrische data.

Opdat dit verbod van toepassing zou zijn, is de plaats van toepassing het gebied van de 'werkplek', wat—op basis van de Commissierichtsnoeren inzake verboden praktijken op het gebied van kunstmatige intelligentie praktijken die zijn vastgesteld bij Verordening (EU) 2024/1689 [*"Richtsnoeren inzake verboden praktijken op het gebied van kunstmatige intelligentie"*)]—ruim moet worden geïnterpreteerd en ook virtuele ruimten omvat (bijv. in het geval van thuiswerk). De tekst van de AI Act noemt niet uitdrukkelijk 'werknemers' als doelwit van dergelijke AI-systemen. In de gerelateerde overweging 44 van de AI Act wordt uitgelegd dat de beperking tot 'werkplek' bedoeld is om de machtsongelijkheid in de context van werk aan te pakken, wat kan suggereren dat het verbod van toepassing is op de inzet van dergelijke AI-oplossingen op 'werknemers'.

Bovendien wordt in de Richtsnoeren inzake verboden AI-praktijken verduidelijkt dat de status van werknemer, contractant, stagiair, vrijwilliger, etc. irrelevant is voor dit verbod en dat het begrip 'werkplek' ook van toepassing moet zijn op kandidaten tijdens het selectie- en wervingsproces. Dit geeft duidelijk aan dat het gebruik van emotieherkennungssystemen al strikt verboden is in het wervingsproces, ook in het geval van online werving van nieuwe 'werknemers', en de lijst met voorbeelden suggereert dat het gebruik van dergelijke systemen alleen verboden is op 'werknemers' (ruim geïnterpreteerd). Bovendien staan in de Richtsnoeren inzake verboden AI-praktijken een aantal richtinggevende voorbeelden van mogelijk verboden gebruik van emotieherkennungssystemen. Het gebruik van dergelijke systemen om de emoties van werknemers tijdens telefoongesprekken met klanten te identificeren, is verboden.

Bovenstaande interpretatie is belangrijk, omdat de zuiver grammaticale interpretatie van deze bepaling van de AI Act zou kunnen leiden tot een brede toepasbaarheid van de bepaling, waarbij iedereen die zich toevallig op de werkvloer bevindt (bijvoorbeeld cliënten die een notariskantoor binnengaan), eronder zou vallen. Echter, in overeenstemming met een praktijkvoorbeeld van de Richtsnoeren inzake verboden AI-praktijken is het gebruik van camera's in een supermarkt of bank om verdachte klanten op te sporen (bijvoorbeeld klanten die op het punt staan een overval te plegen) niet verboden onder het relevante artikel van de AI Act zolang het zeker is dat er geen werknemers worden gevolgd. Zodoende kan het verbod zo worden uitgelegd dat het niet van toepassing is op gevallen waarin emotieherkennungstechnologieën worden toegepast op cliënten in notariskantoren.

Het niet-verboden gebruik van emotieherkennungssystemen valt onder de hoge risicocategorie, met bijzondere transparantieplichtingen.

Om inbreuken op de bescherming van persoonsgegevens te voorkomen moeten de relevante bepalingen van de AVG strikt worden nageleefd.

Dit voorbeeld laat in ieder geval zien dat de toepasbaarheid van alle regels van de AI Act—ook al is het onwaarschijnlijk dat de betreffende situaties zich in de praktijk zullen voordoen—altijd moet worden geverifieerd.

b) AI-systemen met een hoog risico

Volgens de AI Act zijn systemen die onder deze classificatie vallen systemen die een nadelig effect kunnen hebben op de gezondheid, veiligheid en grondrechten van personen.

De AI Act introduceert twee hoofdcategorieën op basis waarvan een bepaald AI-systeem kan worden geclassificeerd als hoog risico. De eerste—die geen betrekking heeft op het notariaat—omvat AI-systemen die bedoeld zijn om te worden gebruikt als veiligheidscomponenten van een product of die zelf producten zijn, vallen onder de EU-harmonisatiewetgeving in bijlage I van de AI Act, en het product of het AI-systeem moet een conformiteitsbeoordeling door een derde partij ondergaan. Dit zijn bijvoorbeeld autonome robots, zelfrijdende auto's of medische diagnoseapparatuur.

Bijlage III van de AI Act omvat de andere groep gebieden en criteria, volgens welke een bepaald AI-systeem onder de categorie hoog risico kan vallen. De verlening van juridische diensten komt niet voor in bijlage III, maar op basis van de bevoegdheden en activiteiten in de EU kunnen twee punten uit die bijlage worden geïdentificeerd op basis waarvan we moeten bekijken of de AI-systemen die (mogelijk) door het notariaat op die gebieden en onder die omstandigheden worden gebruikt, onder de risicocategorie vallen.

Het eerste is punt 1. c): de biometrische AI-systemen bedoeld om te worden gebruikt voor emotieherkenning. Volgens overweging 44 van de AI Act zijn emotieherkenningssystemen AI-systemen die emoties of bedoelingen van natuurlijke personen identificeren of afleiden op basis van hun biometrische data. Zoals eerder vermeld in hoofdstuk III over de mogelijke gebruikssituaties van AI-systemen door notarissen, met name in notariële procedures op afstand, kunnen AI-oplossingen voor emotieherkenning en sentiment-analyse de relevante menselijke (notariële) vaardigheden aanvullen en de notarissen helpen om een gefundeerde beslissing te nemen, bijvoorbeeld over de vraag of de cliënt aan de andere kant van het videogesprek bedreigd wordt of onder druk staat. Zelfs als het niet wordt aanbevolen dat de notaris zijn/haar beslissing uitsluitend neemt op basis van de aanbevelingen van dergelijke systemen, kan alleen al het gebruik ervan leiden tot een indeling in de categorie hoog risico.

Het is belangrijk om op te merken dat onder hetzelfde punt—subpunt a)—alleen de biometrische identificatiesystemen op afstand als hoog risico worden aangemerkt. AI-systemen die bedoeld zijn om te worden gebruikt voor biometrische verificatie met als enig doel te bevestigen dat een specifieke natuurlijke persoon de persoon is die hij/zij beweert te zijn en om de identiteit van een natuurlijke persoon te bevestigen met als enig doel toegang te krijgen tot een dienst, vallen buiten de categorie met een hoog risico. Daarom wordt de biometrische verificatie door de notaris met behulp van AI bij procedures op afstand niet als een hoog risico beschouwd.

Het tweede punt dat van belang kan zijn voor de notariële beroepsgroep is punt 8 a), waar in de categorie met een hoog risico het volgende wordt geschaard: *‘AI-systemen die bestemd zijn om door of namens een rechterlijke instantie te worden gebruikt om een rechterlijke instantie bij te staan bij het onderzoek en de interpretatie van feiten en het recht en bij de toepassing van het recht op een concrete reeks*

feiten, of om op soortgelijke wijze te worden gebruikt bij alternatieve geschillenbeslechting’. Deze bepaling kan slechts betrekking hebben op het deel van de leden van de CNUe die worden beschouwd als ‘gerechtelijke autoriteiten’ of entiteiten die namens een gerechtelijke autoriteit optreden. Deze bepaling kan bijvoorbeeld van invloed zijn op de notarissen van Hongarije, die optreden als gerechtelijke autoriteiten (als rechters in eerste aanleg) in erfrechtprocedures, of de notarissen van Oostenrijk, die optreden als gerechts-commissarissen (*‘Gerichtskommissär’*). Als notarissen met een status in een van de twee voorgaande categorieën gebruikmaken van een AI-systeem voor het onderzoeken en interpreteren van feiten en de wet, en bij het toepassen van de wet op een concrete reeks feiten, kan hun gebruik in de categorie met een hoog risico vallen. Als zo’n notaris bijvoorbeeld AI-oplossingen gebruikt om de bankrekeningen van de overledene op te zoeken (onderzoek naar een feit), om jurisprudentie over bepaalde wetsbepalingen te achterhalen om deze correct te interpreteren (onderzoek en interpretatie van de wet) of om een nalatenschapsbeslissing op te stellen op basis van de feiten van de zaak (toepassing van de wet op een concrete reeks feiten), kan zijn/haar gebruik van AI in de categorie met een hoog risico vallen. Hetzelfde kan van toepassing zijn als een notaris die de status van gerechtelijke autoriteit heeft of namens deze optreedt, optreedt als bemiddelaar (een vorm van alternatieve geschillenbeslechting) en daarvoor gebruik maakt van bepaalde AI-systemen. De AI Act bevat een groot aantal situaties waarin het gebruik is vrijgesteld van hoog risico. Het is daarom niet zeker of bovenstaande voorbeelden uiteindelijk als risicovolle gevallen zullen worden beschouwd.

Bij de interpretatie van deze bepalingen moet er rekening mee worden gehouden dat ze pas vanaf 2 augustus 2026 van toepassing zijn en dat er dus tot die tijd geen jurisprudentie is waarin de inhoud ervan duidelijk naar voren komt. Van de kant van de Europese Commissie worden enkele relevante praktische richtlijnen verwacht, maar ten tijde van het schrijven van dit Handboek zijn deze nog niet gepubliceerd. Daarom kan de beroepsgroep de relevante bepalingen alleen interpreteren op basis van hun grammaticale betekenis en de bijbehorende overwegingen die de bedoeling van de wetgever benadrukken. In overweging 61 worden bijvoorbeeld *‘rechters’* en *‘rechterlijke afhankelijkheid’* genoemd, maar de classificatie van notarissen als rechterlijke autoriteiten of handelend namens hen in bepaalde rechtssystemen suggereert dat AI-gebruik door die notarissen in de relevante gevallen ook onder de categorie

met een hoog risico kan vallen. Ook de uitdrukking “bestemd om te worden gebruikt” is aan interpretatie onderhevig, aangezien het niet duidelijk is wat de toepasselijke classificatie is als een AI-systeem niet bedoeld is om te worden gebruikt voor de in bijlage III genoemde doeleinden, maar in feite wel zo wordt gebruikt.

c) Uitzondering op de categorie voor hoog risico

In overeenstemming met de AI Act [artikel 6 lid 3] zijn er uitzonderingen of afwijkingen, waardoor wat anders onder de AI Act als een systeem met hoog risico wordt gezien, niet als zodanig wordt beschouwd. Deze zijn als volgt: *‘een AI-systeem als bedoeld in bijlage III wordt niet beschouwd als hoog risico wanneer het geen aanmerkelijk risico inhoudt dat de gezondheid, de veiligheid of de grondrechten van natuurlijke personen worden geschaad, onder meer doordat het resultaat van de besluitvorming niet wezenlijk wordt beïnvloed. De eerste alinea is van toepassing wanneer aan een van de volgende voorwaarden is voldaan:*

- (a) het AI-systeem is bedoeld om een ‘smalle’ procedurele taak uit te voeren;*
- (b) het AI-systeem is bedoeld om het resultaat van een eerder voltooide menselijke activiteit te verbeteren;*
- (c) het AI-systeem is bedoeld om besluitvormingspatronen of afwijkingen van eerdere besluitvormingspatronen te detecteren en niet bedoeld om de eerder uitgevoerde menselijke beoordeling te vervangen of te beïnvloeden, zonder passende menselijke beoordeling; of*
- (d) het AI-systeem is bedoeld om een voorbereidende taak uit te voeren voor een beoordeling die relevant is voor de in bijlage III genoemde gebruikssituaties.”*

Als een AI-systeem wordt ontwikkeld of ingezet door het notariaat onder de categorie hoog risico moet worden onderzocht of een van de bovenstaande uitzonderingen van toepassing is. In deze gevallen achtte de wetgever het risico van aantasting van de grondrechten van natuurlijke personen zo gering dat het niet nodig werd geacht om de verplichtingen toe te passen die zijn vastgelegd voor AI-systemen met een hoog risico. Heel belangrijk is dat dit het geval is wanneer het AI-systeem een materiële invloed heeft op de beslissing van de gebruiker.

Er zijn verschillende zaken uit het notariaat die vermoedelijk onder deze uitzonderingen zouden vallen. Zo is het verzamelen van de gegevens van de erfgenamen uit de

elektronische documenten met betrekking tot erfrechtzaken om ze rechtstreeks over te brengen naar het concept van de notariële erfrechtbeslissing een smalle procedurele taak. In het geval dat het wordt geautomatiseerd door AI, kan de eerste uitzondering van toepassing zijn en kan het systeem worden beschouwd als niet-hoog-risico. Bovendien, als de notaris een AI-tool gebruikt dat de kwaliteit van zijn/haar beslissing kan verbeteren door typefouten en grammaticale fouten te verwijderen bij het citeren van de relevante wettelijke bepalingen, kan de tweede uitzondering zeker van toepassing zijn. Bovendien kan onder de derde categorie het gebruik vallen van een AI-systeem dat de notaris helpt bij het detecteren van afwijkingen van zijn/haar soortgelijke eerdere beslissingen en de notaris waarschuwt voor deze afwijkingen. Tot slot, bij het toepassen van AI-oplossingen om de bankrekeningen van de overledene te doorzoeken, kan dit worden beschouwd als het gebruik van een AI-systeem om een voorbereidende taak uit te voeren voor een beoordeling die relevant is voor het opstellen van een nalatenschapsbeslissing. Als de notaris echter de feiten invoert in een generatieve AI-oplossing om een geautomatiseerd eerste ontwerp van zijn/haar beslissing te creëren, is de bovenstaande uitzondering hoogstwaarschijnlijk niet van toepassing en wordt het gebruik van het systeem als hoog risico beschouwd.

Bij de beoordeling van de uitzonderingen moet de notaris uiterst zorgvuldig te werk gaan en per geval bepalen of een van de uitzonderingen van toepassing kan zijn.

Het is belangrijk om hier al te vermelden dat wanneer een notariële organisatie (beroepsorganisatie) een aanbieder is van een AI-systeem met hoog risico dat deze als niet als hoog-risico beschouwt, deze de desbetreffende beoordeling documenteert voordat het systeem in gebruik wordt genomen [artikel 6, lid 4]. Bovendien moet, voordat een dergelijk systeem in gebruik genomen wordt, de notariële aanbieder in ieder geval het betreffende systeem registreren in de EU-databank die moet worden opgezet op basis van de AI Act [ook artikel 6 lid 4]. De registratieplicht geldt ook voor gebruikers van systemen met hoog risico die overheidsinstanties zijn (bijv. notarissen als zij als zodanig worden beschouwd door hun respectieve wetgeving) of personen die namens hen handelen. Deze registratie (gebruiker, entiteit, gebruik) moet worden uitgevoerd voordat het betreffende systeem gebruikt wordt [artikel 71, lid 3].

d) Bepaalde AI-systemen met transparantieplichtingen

De AI Act bevat een lijst van AI-systemen die onder deze categorie kunnen vallen (artikel 50). Omdat het breder is dan de mogelijke gebruikssituaties binnen het notariaat, is het vooraf gestuurde subpunt slechts gericht op twee relevante bepalingen, namelijk de ontwikkeling en het gebruik van chatbots en de inzet van emotieherkennings-systemen.

Chatbots kunnen door de notariële organisaties en individuele notarissen worden aangeboden aan (potentiële) klanten voor verschillende doeleinden (bijvoorbeeld om eenvoudige vragen over de wet te beantwoorden, een notaris te vinden, een afspraak te maken met een notariskantoor). Gebaseerd op de relevante bepalingen van de AI Act [Artikel 50 lid 1] moeten de aanbieders van dergelijke systemen die bedoeld zijn voor rechtstreekse interactie met natuurlijke personen de systemen zodanig ontwerpen en ontwikkelen dat de betrokken natuurlijke personen ervan op de hoogte zijn dat ze te maken hebben met een AI-systeem. Een dergelijke informatieverplichting geldt niet als het vanuit het standpunt van een redelijk geïnformeerde, omzichtige en oplettende natuurlijke persoon duidelijk is dat die persoon in interactie is met een AI-systeem. Voor de veiligheid van de aanbieder en de gebruiker is het sterk aan te raden om altijd aan te geven dat de (potentiële) cliënt interacteert met een AI-systeem.

Verschillende artikelen in de AI Act gaan over emotieherkenningssystemen. Zoals hierboven vermeld zijn emotieherkenningssystemen op de werkplek (bijv. in notariskantoren) in principe verboden. Bovendien—wanneer het verbod niet van toepassing is—vallen deze systemen ook onder de categorie van hoog risico. Tot slot schrijft het relevante artikel [artikel 50, lid 3] over de specifieke transparantieplichtingen van bepaalde AI-systemen voor dat gebruikers van een emotieherkenningssysteem de natuurlijke personen die eraan worden blootgesteld moeten informeren over de werking van het systeem en moeten de gebruikers de persoonsgegevens verwerken in overeenstemming met de AVG. In de notariële praktijk—zoals eerder genoemd—kan door het potentiële gebruik van emotieherkenningssystemen binnen de procedure voor

het opstellen van notariële akten op afstand (via videobellen) deze verplichting tot transparantie en bescherming van persoonsgegevens in werking treden.

De AI Act bepaalt de manier waarop deze informatie moet worden verstrekt aan de getroffen natuurlijke personen: dit moet op een duidelijke en onderscheidbare manier gebeuren en moet worden uitgevoerd op het moment van de eerste interactie en blootstelling met de betreffende natuurlijke persoon.

e) AI-systemen met een minimaal risico

Deze categorie wordt niet gedefinieerd of genoemd in de AI Act, maar bestaat als categorie 'AI met een minimaal risico' in theorie en in de praktijk aantoonbaar wel. De AI Act schrijft zelf geen verplichtingen voor die van toepassing zijn op systemen die niet onder de categorie hoog risico of onder de categorie waarvoor transparantieplichtingen moeten worden nagekomen vallen. Daarom vallen AI-oplossingen—zelfs als ze worden gebruikt op het gebied van rechtspleging—als ze niet onder een van de twee voorgaande categorieën vallen, ook niet onder het materiële toepassingsgebied van de AI Act. Dit betekent echter niet dat ze volledig vrij van risico zijn. Zoals vermeld in de verschillende hoofdstukken van dit Handboek, kunnen er verschillende risico's optreden bij het gebruik van dergelijke systemen. Als dergelijke oplossingen niet op de juiste manier worden gebruikt, kunnen ze bijvoorbeeld inbreuk maken op de privacy en persoonsgegevens, beroepsgeheim, etc.

In de notariële praktijk kunnen veel AI-oplossingen worden ingedeeld in de categorie minimaal risico, waarvoor de AI Act niet van toepassing is. De AI-oplossingen voor de anonimisering van notariële akten en beslissingen, AI-systemen voor afspraakreservering, spraak-naar-tekst tools, hulpmiddelen voor het samenvatten van documenten, etc. kunnen onder deze categorie vallen. In principe, wanneer een AI-systeem met hoog risico valt onder de uitzondering, tenzij specifieke transparantie bepalingen onder de AI Act van toepassing zijn, moet worden nagegaan wat voor soort risico's uit de AI Act moeten worden aangepakt.

5. Wat te doen als een notarieel AI-systeem in de categorie hoog risico valt?

De AI Act schrijft uitgebreide nalevingsverplichtingen voor aan zowel de aanbieders en de gebruikers van AI-systemen met een hoog risico. Deze verplichtingen vereisen vaak extra personeel en aanzienlijke financiële middelen. Wanneer de mogelijkheid bestaat om AI-oplossingen te introduceren die onder de categorie hoog risico vallen, moeten de notariële organisatie en de notarissen beoordelen of het voldoen aan de verplichtingen in de AI Act meer of minder belastend zou zijn dan wanneer er andere middelen worden ingezet die niet onder de categorie AI vallen of niet onder de categorie hoog risico. Deze beslissing is met name belangrijk omdat de AI Act geldelijke sancties voorschrijft met hoge maximumbedragen in geval van niet-nakoming van de respectieve verplichtingen (bijv. 15 miljoen euro in geval van niet-nakoming van de verplichtingen van aanbieders en gebruikers).

i) De verplichtingen van de aanbieders van AI-systemen zijn als volgt:

- Het opzetten, implementeren, documenteren en onderhouden van een risicobeheersysteem voor de voortdurende bewaking en beperking van potentiële risico's (artikel 9);
- Het waarborgen van de kwaliteit en relevantie van gegevens met betrekking tot training, validatie en testgegevens (artikel 10);
- Opstellen en regelmatig bijwerken van technische documentatie (met de elementen in bijlage IV) voor nalevingscontrole (artikel 11);
- Opzetten van een automatische archiveringsfunctie, die de gebeurtenissen (logs) registreert gedurende de levensduur van het systeem, waarbij de automatisch gegenereerde logbestanden ten minste zes maanden worden bewaard (artikelen 12 en 19);
- Zorgen voor transparantie van de AI-operatie zodat gebruikers de outputs en gebruiksinstructies van een systeem kunnen interpreteren om het AI-systeem op de juiste manier in te zetten (artikel 13);
- Efficiënt menselijk toezicht voor de bewaking van het AI-systeem en om zo nodig in te grijpen (artikel 14);

- De nauwkeurigheid, robuustheid en cyberveiligheid van het systeem zodat het veilig en nauwkeurig is en bestand tegen aanvallen (artikel 15);
- Opzetten van een kwaliteitsmanagementsysteem (schriftelijk beleid, procedures, instructies) voor het waarborgen van de naleving van de AI Act (artikel 17);
- De relevante documenten (bv. technische documentatie, documenten over het kwaliteitsbeheer) gedurende 10 jaar nadat het AI-systeem in gebruik is genomen ter beschikking houden van de nationale bevoegde autoriteiten (artikel 18);
- Onmiddellijk de nodige corrigerende maatregelen nemen om het AI-systeem in overeenstemming te brengen, in te trekken, uit te schakelen of terug te roepen bij een vermoeden van niet-naleving van de AI Act; daaropvolgende verstrekking van informatie aan de gebruikers (artikel 20);
- Het verstrekken van informatie aan de bevoegde autoriteit (inclusief de automatisch gegenereerde logbestanden) en documentatie die de conformiteit van het AI-systeem met de AI Act aantoont, na een gemotiveerd verzoek (artikel 21);
- Een conformiteitsbeoordeling uitvoeren om aan te tonen dat het AI-systeem voldoet aan de verplichte eisen voor betrouwbare AI. De conformiteitsbeoordeling moet worden herhaald als het systeem of het doel daarvan wezenlijk wordt gewijzigd (artikel 43); het opstellen van een AI-verklaring van conformiteit met de inhoud van bijlage V van de AI Act (artikel 47);
- Registratie van het AI-systeem in de EU-databank (artikel 49);
- Zorgen voor voldoende AI-kennis bij het personeel en andere personen die namens hen te maken hebben met de werking en het gebruik van AI-systemen (artikel 4).

ii) De verplichtingen van de gebruikers van AI-systemen zijn als volgt:

- Passende technische en organisatorische maatregelen nemen om ervoor te zorgen dat ze dergelijke systemen gebruiken in overeenstemming met de gebruiksaanwijzingen bij de systemen en dat zij bevoegde personen aanwijzen met menselijk toezicht en ondersteuning (artikel 26, punten 1 en 2);

- Voor zover de gebruiker controle uitoefent over de inputgegevens, het toepassen van gegevenscontrole om te waarborgen dat de inputgegevens relevant en voldoende representatief zijn met het oog op het beoogde doel van het AI-systeem (artikel 26, punt 4);
- Het bewaken van de werking van het AI-systeem op basis van de gebruiksinstructies, het geven van feedback en informatie aan de aanbieders en de bevoegde autoriteiten in vooraf bepaalde gevallen (bv. een ernstig ongeval) (artikel 26, punt 5);
- De automatisch gegenereerde logbestanden gedurende ten minste zes maanden bewaren, voor zover de gebruiker daar controle over heeft (artikel 26, punt 6);
- In het geval dat de gebruiker een werkgever is (bv. een notaris), moet hij/zij de betrokken werknemers (bv. notariskandidaten, administratief personeel) informeren dat zij zullen worden onderworpen aan het gebruik van het AI-systeem met hoog risico (artikel 26, punt 7);
- In het geval dat de gebruiker een overheidsinstantie is (zoals het geval kan zijn voor notarissen krachtens hun respectieve nationale wetgeving), moet hij/zij/het zichzelf registreren in de bovengenoemde EU-databank en controleren of het te gebruiken systeem geregistreerd is (zo niet, dan kan het systeem niet gebruikt worden en moet de aanbieder ingelicht worden) (artikel 26, punt 8);
- Als het AI-systeem beslissingen neemt of helpt bij het nemen van beslissingen met betrekking tot natuurlijke personen, informeert de gebruiker de natuurlijke personen dat zij onderworpen zijn aan het gebruik van een AI-systeem met hoog risico (artikel 26, punt 11);
- Samenwerking met de relevante bevoegde autoriteiten (artikel 26, punt 12);
- Zorgen voor voldoende AI-kennis bij hun personeel en andere personen die namens hen te maken hebben met de werking en het gebruik van AI-systemen (artikel 4).

Voordat een AI-systeem met hoog risico wordt ingezet moeten de gebruikers die een publiekrechtelijke instelling zijn of een particuliere instelling die openbare diensten verleent, een beoordeling uitvoeren van de gevolgen die het gebruik van een dergelijk systeem kan hebben voor de grondrechten (beoordeling van gevolgen voor de grondrechten – FRIA, artikel 27). De FRIA moet worden ingelicht wanneer de gebruiker van mening is dat een van de relevante factoren is veranderd. Het AI Office (opgericht binnen de Europese Commissie) zal een sjabloon voor een vragenlijst ontwikkelen om gebruikers te helpen om gemakkelijk te voldoen aan hun verplichtingen met betrekking tot de FRIA. Zodra de FRIA is uitgevoerd, informeert de gebruiker de bevoegde markttoezichtautoriteit over de resultaten.

Op basis van de formulering van dit artikel is het onzeker of notariële organisaties en notarissen onder deze verplichting vallen wanneer ze AI-systemen met een hoog risico gebruiken. Het risico bestaat dat notariële organisaties onder deze clause vallen, omdat ze in veel landen onder het publiekrecht vallen. Bovendien kunnen notarissen in bepaalde lidstaten worden beschouwd als particuliere entiteiten die openbare diensten verlenen. Volgens overweging 96 *‘houden particuliere entiteiten die dergelijke openbare diensten verlenen, verband met taken van algemeen belang, zoals op het gebied van onderwijs, gezondheidszorg, sociale diensten, huisvesting, rechtsbedeling’*, wat kan impliceren dat notarissen met een dergelijke status die openbare diensten verlenen in verband met de rechtsbedeling, onderworpen zijn aan FRIA-verplichtingen.

Belangrijkste conclusies

- De AI Act is een rechtstreeks toepasselijke EU-regelgeving en is wereldwijd de eerste uitgebreide reeks wettelijke regels inzake AI en de primaire rechtshandeling die van toepassing is op AI binnen de EU.
- De AI Act zal in principe 24 maanden na de inwerkingtreding volledig van toepassing zijn, oftewel vanaf 2 augustus 2026, maar een deel van de bepalingen zal al eerder gelden.
- De AI Act volgt een risicogebaseerde aanpak op basis waarvan de AI-systemen kunnen worden ingedeeld in 4 categorieën: verboden AI-praktijken, AI-systemen met een hoog risico, bepaalde AI-systemen met transparantieplichtingen en AI-systemen met een minimaal risico.
- Het persoonlijke toepassingsgebied van de AI Act omvat de aanbidders, de gebruikers, de importeurs en distributeurs van AI-systemen.
- Notariële organisaties kunnen worden beschouwd als aanbieders uitsluitend door het ontwikkelen van een AI-systeem, en notarissen kunnen worden beschouwd als gebruikers bij het gebruik van AI-systemen binnen hun professionele activiteiten.
- De kwalificatie van een notariële organisatie en/of een notaris als een 'aanbieder' of gebruiker betekent niet automatisch dat verdere bepalingen van de AI Act ook op hen van toepassing zijn.
- Verboden AI-praktijken zullen waarschijnlijk niet voorkomen in het notariaat, maar de regels die van toepassing zijn op deze praktijken moeten altijd worden nageleefd (bijv. emotieherkenning op de werkplek).
- Bijlage III van de AI Act bevat gebieden en criteria die ook relevant zijn voor het notariaat, volgens welke een bepaald AI-systeem kan vallen onder de categorie hoog risico.
- De twee gevallen waarin een notariële AI-oplossing onder de categorie hoog risico vallen zijn de biometrische AI-systemen voor emotieherkenning (bijv. voor notariële procedures op afstand) en de AI-systemen bedoeld om door of namens een gerechtelijke autoriteit te worden gebruikt om een gerechtelijke autoriteit bij te staan bij het onderzoeken en interpreteren van feiten en het recht en bij het toepassen van het recht op een reeks concrete feiten, of om op soortgelijke wijze te worden gebruikt bij alternatieve geschillenbeslechting.
- Er zijn uitzonderingen opgenomen in de AI Act die ertoe leiden dat niet alle systemen met een hoog risico uiteindelijk als zodanig worden beschouwd. De uitzondering is van toepassing op opgesomde gevallen die situaties omvatten waarin het gegeven systeem geen significant risico inhoudt dat de gezondheid, de veiligheid of de grondrechten van natuurlijke personen worden geschaad, onder meer wanneer het AI-systeem de beslissing van de gebruiker (notaris) niet materieel beïnvloedt.
- Bij de beoordeling van de uitzonderingen moet de notaris uiterst zorgvuldig te werk gaan en per geval bepalen of een van de uitzonderingen van toepassing kan zijn, rekening houdend met het feit dat andere verplichtingen in de AI Act nog steeds van toepassing kunnen zijn.
- De twee AI-systemen die onder specifieke transparantieplichtingen van het notariaat kunnen vallen, zijn de chatbots en de emotieherkenningssystemen. In deze twee gevallen moet de notaris de getroffen persoon (cliënt) informeren dat hij/zij in contact komt met/wordt blootgesteld aan een AI-systeem.
- In de notariële praktijk kunnen we een breed scala aan AI-oplossingen indelen in de categorie met minimaal risico waarvoor de AI Act niet van toepassing is (bijv. AI-systemen voor afspraakreservering, spraak-naar-tekst tools).
- De AI Act schrijft uitgebreide nalevingsverplichtingen voor aan zowel de aanbieders en de gebruikers van AI-systemen met een hoog risico, en hoge geldelijke sancties als deze niet worden nageleefd.

V. Data en artificiële intelligentie

1. Het belang van data voor AI

Datawetenschap is een aparte discipline, maar is tegelijkertijd nauw verbonden met de wetenschap van artificiële intelligentie en er absoluut essentieel voor.

Data kan simpelweg worden vergeleken met de brandstof van motorvoertuigen; op dezelfde manier dat zelfs de meest hoogwaardige voertuigen niet zonder brandstof kunnen, kan AI niet functioneren zonder data. Daarnaast—en dan nemen we nog steeds het voorbeeld van motorvoertuigen—speelt het type brandstof (diesel of benzine) een fundamentele rol in het functioneren van het voertuig. Zodoende kunnen ook AI-systemen voor gebruik door juridische professionals alleen werken met de juiste juridische en ondersteunende gegevens. Aangezien brandstof van lage kwaliteit leidt tot kapotte motoren, leidt de lage kwaliteit van data (*'impaired data'*)—als gevolg van verschillende factoren die hieronder worden besproken—tot een verkeerde werking en output van het betreffende AI-systeem. Net als de effecten van brandstof van lage kwaliteit, worden de effecten van slechte data waarschijnlijk pas zichtbaar na een bepaalde periode, waarin de schade al aanwezig is.

2. Kaders voor datagovernance

Voordat de brandstof klaar is voor gebruik, wordt hij bewerkt om hem beter geschikt te maken voor moderne voertuigen, en dit proces wordt uitgevoerd volgens strenge protocollen. Data gebruikt voor AI-systemen worden ook verwerkt op basis van gevestigde kaders voor datagovernance, waarbij de data wordt opgeschoond om goed genoeg te zijn voor gebruik in AI-systemen. Het opschonen van data op basis van deze kaders stelt ons in staat om een gegevenscorpus te verkrijgen dat vrij is van dubbele (*'de-duplicatie'*) of irrelevante gegevens, structurele fouten (bijv. typfouten) en waarin de problemen van ontbrekende gegevens zijn aangepakt.

Om precies te zijn moeten de kaders voor datagovernance beleid bevatten voor databeheer van de fase van gegevensverzameling tot de verwerking en de opslag van gegevens. Ze moeten onder andere regels voor gege-

vensvalidatie en maatregelen voor de bescherming van de privacy en persoonsgegevens bevatten (vanwege de specifieke kenmerken en het belang komt dit onderwerp in een apart hoofdstuk van het Handboek aan bod). Daarnaast is de kwestie van bias van AI-systemen een probleem dat een van zijn bronnen heeft in de trainingsdata, meestal vanwege de onevenwichtigheid van de gebruikte gegevens (de kwestie van bias wordt ook gepresenteerd in een apart hoofdstuk), en die ook deel moeten uitmaken van de kaders voor datagovernance.

De kaders moeten betrekking hebben op gegevensbeveiliging door maatregelen in te voeren om gegevens te beschermen tegen ongeoorloofde toegang, wijziging of vernietiging. Daarnaast moeten er processen worden ingesteld om de datakwaliteit continu en proactief te verbeteren en te verfijnen. Er moet echter op worden gewezen dat de uitgebreide juridische kennis en beroepservaring niet in AI-systemen kunnen worden verwerkt.

Ook al wordt de gegevensverwerking steeds meer geautomatiseerd, de menselijke rol blijft cruciaal. Daarom moet de *'data literacy'* van het bevoegde personeel van notariële organisaties en notarissen voortdurend worden bijgehouden.

3. AI-trainingsproces met verschillende data

Het trainingsproces van het betreffende AI-model is niet alleen gebaseerd op de trainingsdata maar ook op de zogenaamde validatiedata en testdata. De trainingsfase kan vanuit de fysieke wereld worden vergeleken met studenten van een klas (hier: het AI-model) die hetzelfde materiaal, dezelfde instructies en dezelfde leermethode krijgen. Het trainingsmateriaal kan door alle studenten worden geleerd, maar het is niet zeker dat ze het materiaal allemaal op hetzelfde niveau begrijpen en de geleerde informatie op dezelfde manier kunnen toepassen. Daarom is er de rol van de validatiedata die worden gebruikt om het beste AI-model (*'de beste student'*) te kiezen voor een bepaalde taak. Tot slot biedt testdata ontwikkelaars de mogelijkheid om te controleren hoe nauwkeurig het betreffende AI-model daadwerkelijk is, wat vergeleken kan worden met

de prestaties van de leerlingen op het eindexamen. Voor de objectieve evaluatie van het model kunnen de validatiedata en testdata niet worden samengevoegd.

Tijdens het trainingsproces moeten de problemen van overfitting en underfitting efficiënt worden aangepakt, die beide gedeeltelijk worden veroorzaakt door problemen met data. In het eerste geval moet het worden vermeden dat het AI-model 'te goed' getraind wordt voor een specifieke output en andere outputs mist doordat de trainingsdata te homogeen is. In het laatste geval levert het model alleen in beperkte omstandigheden nauwkeurige resultaten op, bijvoorbeeld bij het gebruik van data uit de echte wereld.

4. De risico's van aangetaste data en kenmerken van geschikte data

Om de rechtszekerheid en betrouwbaarheid van de data te garanderen (en daarmee ook die van het AI-systeem) moeten de volgende kenmerken van de trainingsdata in acht worden genomen en moeten de volgende gegevensverwerkingsactiviteiten worden uitgevoerd. De risico's die samenhangen met aangetaste data zijn ernstig, omdat de kleinste fout een aanzienlijke impact kan hebben op de output van het AI-systeem en op de activiteit van de gebruiker.

De aangetaste dataset kan meerdere gronden en vormen hebben. De meest voor de hand liggende zijn de verouderde data die gegevens weergeven die vroeger correct waren, maar nu niet meer geldig zijn voor het gestelde doel (bijv. ingetrokken rechtshandelingen, daarop gebaseerde jurisprudentie). Een onvolledige dataset wordt gekenmerkt door ontbrekende elementen die het vermogen aantasten van het AI-systeem om nauwkeurige en betrouwbare output te geven. In het geval van misleidende data zijn de gegevens op zichzelf correct, maar vanwege de context leiden ze tot onjuiste conclusies. Het gebruik van verschillende vormen van data kan leiden tot inconsistente gegevens die het AI-algoritme in verwarring brengen. De trainingsdataset met tegenstrijdige gegevens kan ook negatieve uitkomsten veroorzaken. Deze storingen worden meestal veroorzaakt door menselijke fouten, in tegenstelling tot data poisoning, wat in principe kwaadwillig wordt gedaan met de bedoeling om het trainingsproces te schaden zodat het systeem een onbetrouwbare output levert.

Voor de efficiënte training en betrouwbare werking van AI-systemen moet de trainingsdata nauwkeurig, volledig

[voldoende hoeveelheid], relevant en consistent zijn. Vroegtijdige opsporing en correctie van onwenselijke data is cruciaal voor een betrouwbare werking van het AI-systeem. Daarom is de regelmatige controle, bewaking en bijwerking van de trainingsdata noodzakelijk. Indien nodig worden dataprofessionals (bijv. datawetenschappers) en andere professionals (bijv. linguïsten) ingezet om de trainingsdata zo geschikt mogelijk te maken voor het doel van het betreffende AI-systeem.

5. Interne notariële data en externe databronnen

In het kader van hun activiteiten produceren en verwerken notarissen en notariële organisaties dagelijks aanzienlijke hoeveelheden data. Dit 'notariële datacorpus' kan een perfecte maar onbewerkte basis vormen voor de training van AI-systemen die worden ontwikkeld en/of gebruikt door de beroepsgroep. Naast deze interne data is het onvermijdelijk om gebruik te maken van externe data die verzameld moeten worden uit betrouwbare gegevensbronnen en met strikte inachtneming van de relevante wettelijke beperkingen.

Voorals het gebied van recht is het gebruik van externe databanken met de meest recente versies van Europese, nationale, regionale en lokale rechtshandelingen en jurisprudentie noodzakelijk om betrouwbare resultaten te verkrijgen. Het beheer van externe datasets is cruciaal omdat we in dit geval vaak te maken hebben met reeds verwerkte, opgeschoonde en gecategoriseerde gegevens die de behoeften weerspiegelen van de personen en entiteiten die rechten hebben op die gegevens, met beperkte controle of gebrek aan controle door externe gebruikers. Dezelfde kwaliteitsnormen moeten echter worden gehandhaafd als in het geval van intern verzamelde data, onafhankelijk van de regels en normen waaraan de personen en entiteiten met rechten op die data zijn onderworpen. Als niet aan deze kwaliteitsnormen wordt voldaan, moeten er stappen worden ondernomen om de data aan de bovenstaande eisen te laten voldoen of, als dit niet mogelijk is, om het gebruik van dergelijke externe datasets simpelweg te negeren.

Daarnaast moeten de verschillende regels voor intellectueel eigendom, met name auteursrecht (in detail gepresenteerd in een afzonderlijk hoofdstuk) en voorwaarden die het gebruik bepalen van data waarop anderen rechten hebben, grondig worden nageleefd om juridische geschil-

len te vermijden voor ongeoorloofd gebruik van gegevens en auteursrechtelijk beschermde werken.

Bij het verzamelen de verschillende trainingsdata uit externe bronnen moet, om de relevantie van de data te garanderen, serieus rekening worden gehouden met de taal. Zelfs als de omvang van de beschikbare dataset in grotere talen (zoals Frans, Duits of Spaans) van nature groter is dan in kleinere talen (zoals Hongaars), is het opbouwen van notariële trainingsdatasets van voldoende omvang in die talen ook mogelijk. Tegelijkertijd moet men bij het samenstellen van datasets in grotere talen, vanuit het oogpunt van de taal, uiterst voorzichtig zijn om geschikte bronnen te gebruiken voor verschillende trainingsdoelstellingen, omdat dezelfde taal de officiële taal kan zijn in twee of meer landen met verschillende rechtssystemen. De datasets die relevant zijn voor verschillende landen, rechtssystemen en concepten kan gemakkelijk resulteren in foute resultaten (bijv. Oostenrijkse AI-tools die zijn getraind op Duitstalige gegevens die afkomstig zijn uit Duitsland of Zwitserland).

De interne en externe gegevens die aan de bovenstaande eisen voldoen, moeten efficiënt geïntegreerd en aan elkaar gekoppeld worden om hun consistentie en interoperabiliteit te garanderen. Dit proces helpt de ontwikkelaars van de AI-systemen om gaten in de gegevens te vullen, mogelijke fouten en tegenstrijdigheden te vinden en deze te elimineren voordat het systeem ze gebruikt om onjuiste of foutieve resultaten te geven.

6. Data in prompts en feedbackloops – de menselijke rol bij het verbeteren van data

Het moet ook benadrukt worden dat naast de kwaliteit van de initiële trainingsdata—en het toegepaste algoritme—de kwaliteit van de prompts (formulering van vragen en instructies) die gebruikers invoeren in het systeem invloed heeft op de kwaliteit en nauwkeurigheid van de geleverde output. Daarom is het belangrijk om de gebruikers van de AI-systemen bewust te maken van de juiste formulering van hun prompts. Als er specifieke stappen nodig zijn voor een bepaald systeem met betrekking tot prompts moeten de gebruikers van dergelijke systemen hierover worden geïnformeerd voordat ze dergelijke systemen gaan gebruiken.

Bovendien kunnen bepaalde AI-systemen die gebruik maken van een ML-algoritme voortdurend leren door ook de inputdata van hun gebruikers te gebruiken. Daarom zijn de juiste gegevens in prompts niet alleen van invloed op de kwaliteit van de specifieke output, maar ook op de betrouwbaarheid en effectiviteit van het hele systeem.

De rol van de mens is daarom zonder twijfel noodzakelijk voor de verbetering van diverse AI-systemen, ook tijdens het gebruik ervan. Het fenomeen van een feedbackloop zorgt voor verfijning van het leerproces van AI door middel van feedback. Als de output van een AI-systeem wordt aangemerkt als incorrect door de gebruiker—bijvoorbeeld via prompts—kan het systeem deze feedback gebruiken en zijn dataset aanpassen. Tegelijkertijd kunnen de fouten in de feedbackloop negatieve gevolgen veroorzaken als de inputdata van onvoldoende kwantiteit of kwaliteit zijn.

Belangrijkste conclusies

- AI kan niet correct functioneren zonder de juiste gegevens.
- De lage kwaliteit van data ('impaired data') leidt tot een verkeerde werking en output van het betreffende AI-systeem.
- Als aangetaste data gebruikt wordt, kan de geringste fout een aanzienlijke invloed hebben op de activiteit van de gebruiker. Vroegtijdige opsporing en correctie van aangetaste data is cruciaal.
- Gegevens gebruikt voor AI-systemen moet worden verwerkt op basis van kaders voor datagovernance met beleid voor databeheer.
- Het trainingsproces van het AI-model is gebaseerd op de trainingsdata, validatiedata en testdata, die allemaal een andere rol hebben.
- De trainingsdata moet nauwkeurig, volledig (voldoende hoeveelheid), relevant en consistent zijn.
- Er moeten interne (bijv. notariële documenten) en externe (bijv. juridische databanken) gegevensbronnen worden gebruikt voor een efficiënte werking van notariële AI-systemen. In beide gevallen moeten de gegevenskwaliteitseisen strikt worden nageleefd.
- De kwaliteit van de prompts (formulering van vragen en instructies) van gebruikers is van invloed op de kwaliteit en nauwkeurigheid van de geleverde output.
- Bepaalde AI-systemen leren ook van de inputdata van hun gebruikers, wat ook het belang benadrukt van de kwaliteit van de gegevens in de prompts van gebruikers.
- Als de output van een AI-systeem wordt aangemerkt als incorrect door de gebruiker, kan het systeem deze feedback gebruiken en zijn dataset aanpassen ('feedback loop').

VI. Bescherming van persoonsgegevens en artificiële intelligentie

1. Algemene inzichten

Notarissen produceren en verwerken elke dag enorme hoeveelheden gegevens tijdens hun werk. Een groot deel hiervan zijn persoonsgegevens, meestal van hun cliënten, maar ook van derde natuurlijke personen (bv. personen die rechten hebben op het onroerend goed in een notariële koop- en verkoopovereenkomst). Zonder uitzondering moeten alle notarissen in de EU de regels van de Algemene Verordening Gegevens-bescherming (AVG) toepassen in hun hoedanigheid van gegevensbeheerder of -verwerker. Hetzelfde geldt voor notariële organisaties die persoonsgegevens verwerken (bijvoorbeeld bij het beheren van notariële registers met dergelijke gegevens van notariële cliënten).

Het doel van dit hoofdstuk is niet om de toepassing van de AVG door notarissen te analyseren, maar om de belangrijkste zaken te benadrukken met betrekking tot de bescherming van persoonsgegevens binnen de context van het gebruik en de ontwikkeling van AI door notarissen. Daarom worden onder de volgende punten alleen de bepalingen van de AVG geanalyseerd die relevant (kunnen) zijn voor dit specifieke onderwerp.

2. AVG en de AI Act

De AI Act is gericht op het reguleren van verschillende aspecten van AI-systemen en AI-modellen voor algemene doeleinden volgens een risico gebaseerde aanpak. Het doel van de AVG is anders: de bescherming van de persoonsgegevens van natuurlijke personen (en daarmee van de personen zelf) binnen (en in bepaalde gevallen ook buiten) het grondgebied van de EU. Met andere woorden, de AI Act reguleert een specifieke technologie, de AVG reguleert de verwerking van een gegevenscategorie. De kwestie van de bescherming van persoonsgegevens is aanzienlijk aanwezig in de ontwikkelingsfase en het gebruik van AI-systemen. Om de meest voor de hand liggende voorbeelden te noemen: de trainingsdataset van een AI-systeem kan persoonsgegevens bevatten, en de input (prompts) en de output van het systeem kunnen ook dergelijke gegevens bevatten.

Aan de ene kant bevat de AI Act nauwelijks specifieke bepalingen over de bescherming van persoonsgegevens. In artikel 3, lid 50, van de AI Act verwezen naar de definitie van persoonsgegevens in de AVG, wat tot gevolg heeft dat er geen verschil is in het concept van deze term binnen de twee wetten. Bovendien stelt artikel 2, lid 7, van de AI Act expliciet dat de AI Act geen afbreuk doet aan de toepasselijkheid van de AVG. Daarom zijn de twee verordeningen, ondanks het feit dat ze verschillende doelen hebben, tegelijkertijd van toepassing en vullen ze elkaar aan. Wanneer het betreffende AI-systeem de verwerking van persoonsgegevens omvat moeten de aanbieders en gebruikers ook voldoen aan hun verplichtingen krachtens de AVG.

Aan de andere kant bevat de AVG geen expliciete verwijzing naar AI-technologie. De reden hiervoor is tweeledig: ten tijde van de invoering was het technologische landschap anders, de mate van ontwikkeling en toepassing van AI-systemen was minder groot (ChatGPT was bijvoorbeeld nog maar een idee). Bovendien is de AVG technologie-neutraal, wat betekent dat het van toepassing is op iedere vorm van verwerking van persoonsgegevens, ongeacht of dat wordt gedaan met een eenvoudige typemachine of met behulp van de meest geavanceerde technologieën, zoals AI. Dit betekent dat de AVG volledig van toepassing is op de verwerking van persoonsgegevens door het gebruik van AI-oplossingen, evenals op de verwerking van dergelijke gegevens tijdens de ontwikkeling van AI-systemen.

De relatie tussen de AVG en de opkomende technologieën is echter nooit vrij van spanningen geweest. Een voorbeeld hiervan is de uitoefening van het recht op wissen ('recht om vergeten te worden') binnen de context van de blockchaintechnologie, die—in haar zuiverste vorm—als een van de belangrijkste kenmerken heeft dat ze onveranderlijk en onuitwisbaar is.

Er doen zich nu al problemen voor en dat zal ook zo blijven in verband met AI-technologieën. Persoonsgegevens in het kader van AI worden bijvoorbeeld verwerkt op een manier die overeenkomt met de beginselen van de AVG, zoals gegevensminimalisatie en doelbeperking. Dit kan in sommige gevallen behoorlijk lastig zijn, omdat de essentie

van verschillende AI-oplossingen (bijv. LLM's) juist het gebruik van grote datasets is voor verschillende doeleinden (voorspellingen, inhoud genereren, enz.). Bovendien is het bestaan van de juiste rechtsgrond voor verwerking cruciaal in verband met de training van AI-systemen, wat ongetwijfeld valt onder de brede definitie van 'verwerking' (*'een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;*' – artikel 4, lid 2, van de AVG).

De relatie tussen AI en gegevensbescherming vereist mogelijk een andere aanpak, diepgaande reflectie en een hoge mate van voorzichtigheid van de notariële beroepsgroep.

In 2024 is een intensieve periode van wetgeving (waaronder de AI Act) op EU-niveau afgesloten, en ondanks verzoeken om de AVG aan te passen aan het AI-tijdperk, hebben de EU-instellingen geen plannen in die richting. Ze willen zich eerder richten op de uitvoering van de bepalingen die momenteel van kracht zijn in de context van AI. Verwacht wordt dat er verklarende documenten en richtsnoeren zullen worden uitgegeven, maar deze kunnen het notariaat slechts beperkte specifieke hulp bieden. Onder de volgende punten vindt u een overzicht van de belangrijkste gegevensbeschermingskwesties waaraan notariële organisaties en notarissen aandacht moeten besteden bij het ontwikkelen en/of inzetten van AI-systemen. Over de relatie tussen AI en gegevensbescherming lopen de meningen van professionals (praktijkmensen, wetenschappers, etc.) uiteen. Daarom wordt in geval van twijfel aangeraden om de bevoegde gegevensbeschermingsautoriteiten te raadplegen voordat met de betreffende activiteit wordt begonnen.

3. Verschillende wetgeving – verschillende rollen

Zoals vermeld onder het vorige punt, vullen de AVG en de AI Act elkaar aan en moeten ze hand in hand worden toegepast. De twee wetten werken echter met verschillende categorieën actoren die onder hun toepassingsgebied vallen.

Voor het notariaat worden de categorieën 'aanbieder' en 'gebruiker' als belangrijk aangemerkt door de AI Act. Hoofdstuk IV van dit Handboek bevat een uitgebreide analyse van deze verschillende rollen; daarom worden de relevante verklaringen hier niet herhaald.

In de AVG zijn de categorieën gegevensbeheerder en gegevensverwerker relevant voor het notariaat. Overeenkomstig artikel 4, lid 7, van deze verordening wordt onder 'verwerkingsverantwoordelijke' verstaan *'een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt'*. Punt 8 van hetzelfde artikel geeft de definitie van 'verwerker', waaronder wordt verstaan *'een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt'*.

Net zoals dat de verplichtingen van aanbieders en gebruikers onder de AI Act verschillend zijn, zijn de verplichtingen van verwerkingsverantwoordelijken en verwerkers ook verschillend. Bovendien moeten de respectieve rollen altijd per geval en in overeenstemming met de toepasselijke wetgevingstekst worden vastgesteld (AI Act en AVG). Met andere woorden, het feit dat een notaris onder de categorie van 'gebruiker' valt volgens de AI Act betekent niet direct dat hij/zij een 'gegevensverwerker' is volgens de AVG. Op dezelfde manier, als een notariële organisatie de 'aanbieder' is van het betreffende AI-systeem volgens de AI Act, kan niet direct worden geconcludeerd dat het de 'verwerkingsverantwoordelijke' is volgens de AVG.

Als een beroepsorganisatie bijvoorbeeld persoonsgegevens verwerkt om een specifiek AI-systeem te trainen wordt het beschouwd als een 'aanbieder' volgens de AI Act en een 'verwerkingsverantwoordelijke' volgens de AVG, omdat de beroepsorganisatie het systeem ontwikkelt ('aanbieder') en—in het kader van deze activiteit—beslissingen neemt over de verwerking van persoonsgegevens voor het doel van het trainen van het systeem (verwerkingsverantwoordelijke). Als de beroepsorganisatie vervolgens het specifieke systeem aan notarissen aanbiedt voor hun gebruik, en notarissen gebruiken daarin de persoonsgegevens van hun cliënten, dan zouden de notarissen optreden als 'gebruikers' onder de AI Act en als afzonderlijke 'verwerkingsverantwoordelijken' onder de AVG met betrekking tot de verwerking van de persoonsgegevens van hun cliënten.

(d.w.z. persoonsgegevens die verschillen van de gegevens die zijn gebruikt voor het trainen van het systeem). Zoals onder de volgende punten zal worden geïllustreerd, is dit voorbeeld echter grotendeels fictief en illustreert het slechts een mogelijke scheiding van rollen, omdat dergelijke activiteiten (met name training van AI-systemen met persoonsgegevens) extra activiteiten met zich meebrengen die moeten worden uitgevoerd om inbreuk op/lekken van persoonsgegevens te voorkomen.

4. AVG-beginselen bij AI-gebruik door notarissen

a) Beginselen van de AVG

Een van de belangrijkste boodschappen van dit hoofdstuk is dat de AVG in zijn geheel ook van toepassing is wanneer AI-systemen worden gebruikt in notariële procedures. Dit heeft als direct gevolg dat de beginselen van de AVG ook van toepassing blijven wanneer AI-oplossingen worden ingezet. Deze principes zijn rechtmatigheid, behoorlijkheid en transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid evenals verantwoordingsplicht (artikel 5 van de AVG). Onder de volgende subpunten worden alleen de beginselen besproken die speciale aandacht vereisen.

b) Rechtmatigheid en rechtsgronden van verwerking

Het principe van rechtmatigheid veronderstelt het bestaan van een van de volledig opgesomde rechtsgronden voor verwerking onder Artikel 6 (1) van de AVG. Welke rechtsgrond van toepassing is, hangt af van talrijke factoren, bijvoorbeeld van de status en de rol van de notaris in de betreffende procedure en van de kenmerken en het doel van de specifieke procedure. Aangezien de AVG niet kan worden beschouwd als een nieuw wetgevingsbesluit (het trad bijna 10 jaar geleden, in 2016, in werking), zijn de rechtsgronden voor de notariële verwerking van persoonsgegevens duidelijk en uitgekristalliseerd in alle lidstaten (bijv. toestemming van de betrokken cliënt, nakoming van een wettelijke verplichting, uitoefening van het openbaar gezag). Om na te gaan welke rechtsgrond van toepassing is, moeten de respectieve nationale regels met betrekking tot de gegeven procedure worden geanalyseerd.

De belangrijkste vraag is daarom of het gebruik van AI-systemen binnen deze procedure iets verandert ten

aanzien van deze rechtsgronden (oftewel, zijn er nieuwe verwerkingsgronden nodig wanneer de notaris gebruik maakt van AI-systemen?). Zoals vermeld in verschillende hoofdstukken van dit Handboek, kunnen AI-systemen niet dienen als vervanging van notarissen, maar hen alleen helpen bij hun professionele activiteiten. Daarom is de rol van AI in deze procedures een hulpmiddel dat de essentie en het doel van de procedures niet verandert. Daarom is er voor de inzet van AI-oplossingen in deze context—in principe (zie het volgende subpunt over gevoelige gegevens)—geen wijziging nodig in de rechtsgrond voor de verwerking van de persoonsgegevens (bijv., als de toestemming van de cliënt de rechtsgrond was vóór de toepassing van de AI, dan blijft dat zo).

Bovendien zijn de activiteiten van notarissen gebaseerd op hun bevoegdheden die worden voorgeschreven door de relevante nationale regels. Dit houdt in dat het gebruik van AI door notarissen hun werkzaamheden niet uitbreidt door voorspellingen te doen over of profielen op te stellen van natuurlijke personen, oftewel tot activiteiten die in andere sectoren vaak problematisch blijken te zijn met betrekking tot de verwerking van persoonsgegevens.

c) Verwerking van speciale categorieën persoonsgegevens

De rechtsgronden voor het verwerken van speciale categorieën persoonsgegevens (“*gevoelige gegevens*”) moeten afzonderlijk worden geanalyseerd. De verwerking van dergelijke gegevens kan bijvoorbeeld aan de orde komen bij de inzet van gezichtsherkenning of AI-systemen voor emotieherkenning en sentimentanalyse, die nuttig kunnen zijn om de menselijke beoordeling aan te vullen in het geval van notariële procedures op afstand met behulp van videobellen. Deze technologieën maken gebruik van de biometrische kenmerken (gegevens) van natuurlijke personen en in overeenstemming met artikel 9, lid 1, van de AVG is ‘*de verwerking van biometrische gegevens met het oog op de unieke identificatie van een persoon verboden*’.

Zelfs als de AI Act een duidelijk onderscheid maakt tussen de identificatie en de verificatie van natuurlijke personen, is dit niet het geval met de AVG. Ondanks het ontbreken van een definitie van de twee termen in de laatste verordening, is volgens (niet-bindende) richtlijnen van de Europese Autoriteit voor Gegevensbescherming van 2022 met betrekking tot gegevensbescherming, hetzelfde verbod van toepassing op de verwerking van biometrische ge-

gevens voor de verificatie van de identiteit van een natuurlijke persoon. Het probleem is niet zonder uitzonderingen, maar de rechtsgronden voor verwerking zijn anders dan in het geval van ‘gewone’ persoonsgegevens. In overeenstemming met de huidige tekst van de AVG kan alleen de uitdrukkelijke toestemming van de betrokkene [artikel 9, lid 2, onder b)] de notaris een duidelijke manier geven om te worden bijgestaan door AI-systemen voor het op afstand verifiëren van de identiteit van zijn/haar cliënt.

Hetzelfde geldt echter niet noodzakelijkerwijs voor het gebruik van AI-systemen voor emotieherkenning en sentimentanalyse die de notaris kunnen helpen om zich ervan te vergewissen dat de wil van de cliënt aan de andere kant van het scherm uit vrije wil is gegeven en dat de cliënt niet wordt bedreigd of onder druk wordt gezet. Het verbod op verwerking op basis van artikel 9 heeft alleen betrekking op biometrische gegevens voor de identificatie (en verificatie) van natuurlijke personen en niet op de herkenning en analyse van emoties en gevoelens. Het bepalen van de vrije wil van de cliënt is een integraal onderdeel van notariële procedures en in dit geval kan het AI-systeem de notaris alleen maar helpen om een oordeel te vellen over de wil van de cliënt. Dus zelfs als zulke AI-systemen voornamelijk biometrische gegevens gebruiken, mogen ze niet worden verboden op basis van de regels voor gegevensbescherming. De rechtsgronden voor verwerking betreffende de procedure waarin dergelijke systemen worden ingezet kunnen hetzelfde blijven als zonder de inzet ervan. In dit hoofdstuk moet echter ook worden benadrukt dat dergelijke systemen onder de categorie hoog risico en transparantieverplichtingen vallen volgens de AI Act. Om absolute duidelijkheid te hebben, wordt bovendien vóór de inzet van dergelijke systemen overleg met de bevoegde gegevensbeschermingsautoriteit aanbevolen.

d) Transparantie, integriteit en vertrouwelijkheid

Met betrekking tot transparantie moet de notaris mogelijk aanvullende informatie verstrekken aan de betrokkene wiens gegevens worden verwerkt met behulp van AI (transparantieverplichtingen zijn ook te vinden in de AI Act). Daarom moet de notaris informatie kunnen geven over gegevensverwerking met behulp van AI en ten minste elementaire en begrijpelijke (niet-technische) informatie over hoe deze gegevensverwerking plaatsvindt. In verband met dit beginsel hebben de betrokkenen een uitgebreid recht op informatie (artikel 12).

De informatieverstrekking en de diepgang ervan moeten echter altijd afhangen van de omstandigheden van de zaak en het belang van de rol van het AI-systeem in de procedure. Het kan bijvoorbeeld niet nodig zijn om de cliënt te informeren over het gebruik van automatische vertaalhulp, in het geval dat de notaris dit alleen gebruikt om de procedure te versnellen en hij de definitieve versie van de vertaalde tekst zelf grondig controleert en corrigeert. Omgekeerd kan het nodig zijn om deze informatie te verstrekken bij gebruik van spraak-naar-tekst-oplossingen waarbij de cliënt direct verbonden is met de betreffende AI-tool (de AI detecteert direct de spraak van de cliënt en zet deze om in tekst).

Ten slotte kan de naleving van het transparantiebeginsel problematisch zijn bij het gebruik van *kant-en-klare AI-oplossingen* (bijv. ChatGPT). Zoals beschreven in Hoofdstuk IX—vanwege hun complexiteit—maken deze oplossingen het niet altijd mogelijk voor de gebruikers om hun werking te begrijpen en uit te leggen (black box).

Bij het inzetten van *kant-en-klare oplossingen* kunnen de beginselen van integriteit en vertrouwelijkheid ook niet worden gegarandeerd. Deze AI-oplossingen leren vaak van de prompts van de gebruikers (dat kunnen ook notarissen zijn). Dit houdt in dat bij het geven van cliëntgegevens als input (prompt) aan dergelijke systemen, er een groot risico bestaat dat persoonsgegevens verder worden verwerkt door het specifieke systeem op een onbevoegde en onwetige manier (zulke AI-systemen leren over het algemeen voortdurend van de prompts van de gebruiker), zelfs zonder medeweten van de betrokkene (en de gebruiker van het systeem).

Bovendien kunnen dergelijke persoonsgegevens niet alleen de trainingsdataset van dergelijke systemen vergroten, maar kan de output ervan ook betekenen dat de persoonsgegevens van de cliënt toegankelijk worden voor onbevoegden, wat nog meer problemen oplevert op het gebied van gegevensbescherming. Op basis van de principes van integriteit en vertrouwelijkheid wordt daarom voorgesteld om af te zien van het gebruik van ‘kant-en-klare’ oplossingen in notariële procedures. Hoe dan ook, als de notaris gebruik moet maken van dergelijke AI-systemen is het sterk aan te raden om de persoonsgegevens van de betrokkenen te anonimiseren (zie details hieronder) in de prompt die aan het AI-systeem gegeven wordt, zodat de betrokkene later niet meer kan worden geïdentificeerd.

5. Rechten van de betrokkene bij AI-gebruik door notarissen

a) Rechten van betrokkenen

Naast de beginselen onder het vorige punt bevat de AVG ook specifieke rechten van betrokkenen. Deze zijn als volgt: het recht op informatie, het recht op toegang, het recht op rectificatie, het recht op gegevenswissing ('recht om vergeten te worden'), het recht op beperking van verwerking, het recht op gegevensoverdraagbaarheid, het recht om bezwaar te maken en de rechten (of liever gezegd het verbod) met betrekking tot geautomatiseerde besluitvorming en profilering.

Met betrekking tot AI-gebruik in notariële procedures worden het recht op gegevenswissing en de rechten met betrekking tot geautomatiseerde besluitvorming (ADM) in dit hoofdstuk verder geanalyseerd.

b) Recht op gegevenswissing

De problemen met het recht op gegevenswissing doen zich meestal voor bij het gebruik van 'kant-en-klare' AI-oplossingen. In aanvulling op wat werd gepresenteerd onder het vorige punt met betrekking tot de kwesties van transparantie, integriteit en vertrouwelijkheid, moet worden benadrukt dat zodra persoonsgegevens in de trainingsdataset van dergelijke systemen komen, de betrokkene extreme moeilijkheden kan ondervinden bij het uitoefenen van zijn/haar recht op gegevenswissing. Deze AI-systemen zijn heel vaak LLM's die werken met uitgebreide datasets en complexe algoritmen. Op basis van de huidige technologie is het onmogelijk om zelfs maar één stukje persoonsgegevens te verwijderen zonder het systeem opnieuw te trainen.

Aangezien het doel van de huidige AI-regelgeving niet alleen het waarborgen van de rechten van de betrokken personen is, maar ook het creëren van een innovatievriendelijke omgeving, is het onwaarschijnlijk dat bedrijven die persoonsgegevens op deze manier verplicht zouden worden om hun systemen opnieuw te trainen, aangezien dit een buitensporige extra last en onvoorspelbare gevolgen voor deze entiteiten zou creëren. Op basis van het bovenstaande wordt nogmaals sterk aangeraden om af te zien van het gebruik van persoonsgegevens bij het inzetten van 'kant-en-klare' oplossingen in notariële procedures.

c) Geautomatiseerde besluitvorming

Met betrekking tot ADM schrijft de AVG een standaard verbod voor met verschillende uitzonderingen. Overeenkomstig artikel 22, lid 1, *'heeft de betrokkene het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking, waaronder ook profilering valt, gebaseerd besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem anderszins in aanmerkelijke mate treft'*.

In de context van notariële procedures is de toepassing van dit artikel zeer onwaarschijnlijk. Allereerst moet worden nagegaan of het resultaat van de specifieke notariële procedure een *'beslissing'* is. In het geval van het opstellen van een akte over een onroerendgoedtransactie is het resultaat van de procedure bijvoorbeeld geen beslissing. In sommige niet-gerechtelijke zaken (bijvoorbeeld in erfrechtprocedures in bepaalde landen) neemt de notaris echter een beslissing (vaak gelijkwaardig of vergelijkbaar met gerechtelijke beslissingen).

Bovendien is een van de belangrijkste boodschappen van dit handboek dat notarissen de uiteindelijke beslissers moeten zijn, zelfs als ze de meest betrouwbare en geavanceerde AI-oplossingen gebruiken. Dit betekent dat niet is voldaan aan de voorwaarde van de *'uitsluitend op geautomatiseerde verwerking gebaseerde beslissing'*, aangezien de beslissing niet uitsluitend is gebaseerd op de output van de AI. De menselijke rol in deze procedures is en moet gegarandeerd en zinvol blijven, de notarissen moeten alle details van de output van het AI-systeem controleren voordat ze hun beslissing nemen om de valkuil van automation bias (teveel vertrouwen op de output van AI-systemen) te voorkomen.

6. AVG en ontwikkeling van notariële AI-systemen

a) Dezelfde beginselen en rechten van betrokkenen – verschillende aanpak

Onder Hoofdstuk XII van dit Handboek wordt de prioritering van intern ontwikkelde AI-systemen of extern ontwikkelde AI-systemen op basis van individueel onderhandelde contractvoorwaarden sterk aanbevolen. Op basis van de bovenstaande verklaringen zijn de AVG-beginselen en rechten van betrokkenen ook volledig toepasbaar in het

geval van dergelijke oplossingen, maar vanwege het verschil in doel (het creëren van dergelijke systemen en niet het gebruik van AI voor individuele procedures) zullen de beginselen en rechten van betrokkenen verschillend van toepassing zijn.

b) Doelbeperking en rechtsgrond voor verwerking

Allereerst moeten de doelbeperking en de rechtsgrond voor de verwerking van persoonsgegevens worden geanalyseerd. Zoals eerder vermeld, is het doel van AI bij het gebruik van AI-oplossingen door notarissen om te helpen bij het voltooien van de specifieke notariële taak (bijvoorbeeld het opstellen van een koopcontract). Voor speciale notariële AI-systemen zijn de gegevens die tijdens notariële procedures worden geproduceerd (bijv. gegevens in notariële akten) een van de belangrijkste gegevensbronnen.

Echter—op grond van het beginsel van doelbinding—strekt het doel van de gegevensverwerking zich in individuele gevallen niet uit tot de daaropvolgende training van speciale AI-systemen met de persoonsgegevens van de cliënten van notarissen en andere betrokkenen. Het doel van de gegevensverwerking zal anders zijn dan het oorspronkelijke doel en het risico van verdere verwerking op een manier die niet overeenkomt met het oorspronkelijke doel is aanwezig. Als het gaat om een dergelijke verwerking zullen bovendien de rollen van verwerkingsverantwoordelijke en verwerker hoogstwaarschijnlijk veranderen, afhankelijk van de specifieke omstandigheden (zie hierboven).

Bij het trainen van speciale notariële AI-systemen met behulp van persoonsgegevens kan het bepalen van de toepasselijke rechtsgrond voor verwerking ook problematisch zijn. De cliënt kan toestemming geven voor verdere verwerking ten behoeve van training van AI, maar die toestemming kan op elk moment worden ingetrokken. Een dergelijke terugtrekking kan technische problemen veroorzaken in de werking van het specifieke AI-systeem, aangezien de relevante persoonsgegevens moeten worden verwijderd uit de trainingsdataset, wat kan leiden tot kostbare hertraining van het systeem.

Aangezien notarissen wettelijk niet verplicht zijn om AI-systemen op te zetten kan ook geen beroep worden gedaan op de rechtsgrond van artikel 6, lid 1, onder c) (*‘de verwerking is noodzakelijk om te voldoen aan een wette-*

lijke verplichting die op de verwerkingsverantwoordelijke rust’).

Punt e) van hetzelfde artikel 6, lid 1, lijkt ook problematisch, aangezien het vereist dat de verwerking van gegevens noodzakelijk is voor het uitvoeren een taak van algemeen belang of die deel uitmaakt van de uitoefening van het openbaar gezag van de verwerkingsverantwoordelijke. In dit geval is het zeer de vraag of de training van het AI-systeem (verwerking) noodzakelijk is voor de taak die wordt uitgevoerd in het algemeen belang of in de uitoefening van het openbaar gezag. Het antwoord is waarschijnlijk nee.

De toepassing van artikel 6, lid 1, onder f) (*“gerechtvaardigd belang”*) kan ook worden uitgesloten omdat—afhankelijk van de nationale wetgeving—het notariaat in het algemeen wordt beschouwd als een overheidsinstantie, en de toepassing van de rechtsgrond van gerechtvaardigd belang voor dergelijke verwerkingsverantwoordelijken is uitgesloten.

Bovendien hebben notarissen een geheimhoudingsplicht waaronder ook de persoonsgegevens van hun cliënten vallen. Bij het gebruik van dergelijke gegevens voor de ontwikkeling van notariële AI-systemen bestaat het risico dat de geheimhoudingsplicht van individuele notarissen wordt geschonden (bijv. door de notaris toegang te geven tot de persoonsgegevens van de cliënten van een andere notaris in het ontwikkelde AI-systeem).

Tegelijkertijd moet worden benadrukt dat de bovenstaande uitspraken alleen betrekking hebben op de ontwikkeling van AI-oplossingen voor het notariaat door gebruik te maken van persoonsgegevens. Rekening houdend met de specifieke kenmerken van notariële procedures en mogelijke toepassingen van AI-oplossingen door notarissen (zie Hoofdstuk III), kan worden opgemerkt dat het gebruik van persoonsgegevens voor het trainen van dergelijke systemen niet altijd een cruciale factor is voor de efficiëntie van het AI-systeem. Dit betekent dat AI-systemen voor notarieel gebruik kunnen worden ontwikkeld met behulp van trainingsdata waarin de persoonsgegevens helemaal niet aanwezig of geanonimiseerd zijn, of waarbij de persoonsgegevens van bestaande betrokkenen worden vervangen door synthetische data.

7. Notariële AI buiten het toepassingsgebied van de AVG

a) Gebruik van geanonimiseerde gegevens

Op basis van het bovenstaande zijn de verplichtingen van de AVG van toepassing op notarissen en notariële organisaties die AI-oplossingen ontwikkelen, tenzij ze gegevens gebruiken die buiten het toepassingsgebied van deze verordening vallen. De AVG maakt onderscheid tussen de pseudonimisering en de anonimisering van persoonsgegevens. Gepseudonimiseerde persoonsgegevens kunnen een bepaald beveiligingsniveau bieden, maar de regels van de AVG blijven volledig van toepassing op dergelijke gegevens. Dit is echter niet het geval bij geanonimiseerde gegevens die buiten het toepassingsgebied van de AVG vallen (overweging 26).

Zoals hierboven vermeld, is het gebruik van geanonimiseerde gegevens vooral—maar niet uitsluitend—belangrijk wanneer de notaris van plan is gebruik te maken van ‘kant-en-klare’ AI-oplossingen. Bij AI-systemen met automatische vertalingen kan de notaris bijvoorbeeld vragen (prompt) om een tekst waarin alle persoonsgegevens geanonimiseerd zijn (bijv. door de namen van de partijen bij een koopovereenkomst te vervangen door “verkoper” en “koper” naast de anonimisering en verwijdering van andere persoonsgegevens). De output van het systeem kan vervolgens handmatig worden aangevuld met de relevante persoonsgegevens of met behulp van beveiligde interne softwareoplossingen. Op deze manier wordt het risico van verder gebruik van de persoonsgegevens door de aanbieder van de betreffende AI-dienst efficiënt vermeden.

Hetzelfde geldt voor de ontwikkeling van notariële AI-systemen, maar om andere redenen. Door gebruik te maken van geanonimiseerde persoonsgegevens voor de training van AI-systemen hoeft de aanbieder geen geschikte rechtsgrond voor de verwerking van gegevens te vinden, aangezien deze gegevenscategorie volledig buiten het toepassingsgebied van de AVG valt en er geen risico is van onbedoeld ongeoorloofd gebruik van de betreffende persoonsgegevens door andere notarissen die dit specifieke systeem inzetten.

b) De-anonimisering (her-identificatie)

Het risico van het gebruik van geanonimiseerde gegevens met AI-oplossingen is de mogelijkheid van de-anonimisering (her-identificatie) van dergelijke gegevens. De-anonimisering komt meestal voor wanneer geanonimiseerde gegevens worden gematcht met openbaar beschikbare informatie of aanvullende gegevens, wat leidt tot de identificatie van de persoon van wie de gegevens zijn. Geanonimiseerde gegevens worden weer beschouwd als persoonsgegevens die vallen onder de AVG. In het geval dat ‘kant-en-klare’ oplossingen worden gebruikt en wanneer het risico bestaat dat de-anonimisering kan optreden (bijv. bij het opstellen van akten met specifieke details voor bekende personen van wie de gegevens en informatie op tal van plaatsen online te vinden zijn), is het raadzaam om af te zien van het gebruik van het betreffende AI-systeem, zelfs als daarbij exclusief gebruik wordt gemaakt van geanonimiseerde gegevens.

Bij intern ontwikkelde oplossingen worden passende technische en organisatorische maatregelen genomen om de-anonimisering te voorkomen. Hetzelfde geldt voor extern ontwikkelde notariële AI-oplossingen op basis van contracten waarover afzonderlijk is onderhandeld: de relevante bepalingen moeten een vergelijking bevatten van de aanbieder om de-anonimisering te voorkomen, evenals de passende juridische gevolgen van het schenden van deze verplichting.

c) Synthetische gegevens

Een andere manier om de risico's en problemen rondom het beschermen van persoonsgegevens te voorkomen is het gebruik van synthetische gegevens voor de training van AI-systemen. De AVG bevat geen definitie van en bepalingen over synthetische gegevens, en aangezien deze categorie een nog hoger beveiligingsniveau biedt dan geanonimiseerde gegevens kan worden gesteld dat dergelijke gegevens ook buiten het toepassingsgebied van de AVG vallen. Synthetische gegevens zijn nagebootste trainingsdata, maar omdat er geen specifiek identificeerbare natuurlijke persoon achter zit, is het risico van her-identificatie niet aanwezig. Bovendien is het gebruik van synthetische gegevens ook nuttig als er niet genoeg echte gegevens beschikbaar zijn voor de betreffende AI-training.

d) Persoonsgegevens van overleden personen

Tot slot moet worden opgemerkt dat notarissen—vooral bij het uitvoeren van erfrechtprocedures—een enorme hoeveelheid persoonsgegevens van overleden personen moeten verwerken. In overeenstemming met overweging 27 van de AVG is de verordening niet van toepassing op de persoonsgegevens van overleden personen. Hoewel de AVG niet van toepassing is op persoonsgegevens van overleden personen, laat het de lidstaten vrij om nationale regels op dit gebied in te voeren of om de persoonsgegevens van overleden personen volledig onbeschermd te laten. Daarom moeten de relevante nationale regels worden geraadpleegd om te bepalen hoe deze gegevens kunnen worden verwerkt.

8. Gegevensbeschermingseffectbeoordeling en effectbeoordeling van fundamentele rechten

Zoals vermeld in Hoofdstuk IV, indien gebruikers een publiekrechtelijke instelling zijn of een particuliere instelling die openbare diensten verleent, bevat de AI Act de verplichting om een beoordeling uit te voeren van de gevolgen voor de grondrechten (FRIA – artikel 27 van de AI Act) voordat een AI-systeem met een hoog risico wordt ingezet. De FRIA moet worden bijgewerkt wanneer een van de relevante factoren verandert. Ondanks hun overeenkomsten moet de FRIA niet verward worden met de gegevensbeschermingseffectbeoordeling (DPIA) die verplicht wordt gesteld door de AVG.

Het doel van de FRIA is het vaststellen van de gevolgen voor de grondrechten van individuen of groepen individuen en de maatregelen die moeten worden genomen indien dergelijke rechten worden aangetast door het gebruik van AI-systemen met een hoog risico. Zoals vermeld in Hoofdstuk IV is het onzeker of notariële organisaties en notarissen onder de verplichting vallen om FRIA uit te voeren wanneer zij AI-systemen met een hoog risico inzetten.

Artikel 35 van de AVG bevat de bepalingen over de DPIA. Dit artikel stelt dat de verwerkingsverantwoordelijke in de DPIA de impact moet beoordelen van verwerkingen op de bescherming van persoonsgegevens. De DPIA wordt uitgevoerd wanneer de verwerkingen gebruikmaken van nieuwe technologieën en waarschijnlijk een hoog risico omvatten

voor de rechten en vrijheden van natuurlijke personen. In het geval van AI-gebruik/-ontwikkeling is de belangrijkste vraag of AI kan worden beschouwd als een ‘*nieuwe technologie*’.

Benadrukt moet worden dat de technologische oplossingen die in de huidige AI-producten worden toegepast geen uitvindingen van het laatste decennium zijn; veel ervan vinden hun oorsprong in de tweede helft van de 20e eeuw. Volgens de Richtlijnen voor Gegevensbeschermingseffectbeoordeling door het Europees Comité voor Gegevensbescherming is het gebruik van AI-systemen niet systematisch een toepassing van nieuwe technologische oplossingen. Daarom voldoet niet alle verwerking met behulp van een AI-systeem aan dit criterium en is het noodzakelijk om onderscheid te maken tussen de verschillende systemen. Systemen die bijvoorbeeld gebruik maken van deep learning vallen bijvoorbeeld wel onder de categorie ‘*nieuwe technologie*’.

In dit verband moet er ook rekening mee worden gehouden dat volgens lid 4 van hetzelfde artikel “*de toezichthoudende autoriteit een lijst opstelt van het soort verwerkingen waarvoor een gegevensbeschermingseffectbeoordeling overeenkomstig lid 1 verplicht is, en maakt deze openbaar*”. Het raadplegen van dergelijke lijsten wordt sterk aanbevolen.

Als een notariële organisatie een specifiek notarieel AI-systeem ontwikkelt zonder gebruik van persoonsgegevens/door gebruik te maken van geanonimiseerde of synthetische gegevens, wordt de DPIA niet uitgevoerd, aangezien de AVG niet van toepassing is op deze gegevens. Hetzelfde geldt voor dergelijk AI-gebruik door notarissen.

In geval van verwerking van persoonsgegevens voor AI-ontwikkeling worden de bovengenoemde Richtsnoeren voor Gegevensbeschermingseffectbeoordeling geraadpleegd. In dit document worden 9 criteria opgesomd, en het voldoen aan 2 criteria (bijv. grootschalige verzameling van persoonsgegevens en innovatief gebruik of toepassing van nieuwe technologische oplossingen die in deze context het meest waarschijnlijk zijn) leidt tot het vermoeden dat de DPIA moet worden uitgevoerd. Bij gebruik van AI door notarissen als verwerkingsverantwoordelijken kan met de verwerking van persoonsgegevens het risico van het uitvoeren van een DPIA-beoordeling aanwezig zijn indien het betreffende systeem wordt beschouwd als een

nieuwe technologische oplossing (zie hierboven) en er op grote schaal persoonsgegevens worden verwerkt.

In beide gevallen (ontwikkeling en gebruik) moeten de kenmerken van de specifieke verwerking in overweging worden genomen om een beslissing te nemen over de noodzaak van een DPIA.

Tot slot, als een notariële organisatie of een notaris verplicht wordt om zowel de FRIA als de DPIA uit te voeren, kunnen de twee documenten worden samengevoegd overeenkomstig artikel 27, lid 4, van de AI Act om een uitgebreide analyse te maken.

Belangrijkste conclusies

- De AI Act verwijst naar de definitie van persoonsgegevens in de AVG, wat betekent dat er geen verschil is met betrekking tot de opvatting van deze term binnen de twee wetten.
- Bovendien stelt de AI Act expliciet dat de AI Act geen afbreuk doet aan de toepassing van de AVG.
- De technologisch neutrale AVG is volledig (inclusief de beginselen en de rechten van betrokkenen) van toepassing op de verwerking van persoonsgegevens door het gebruik van AI-oplossingen, evenals op de verwerking tijdens de ontwikkeling van dergelijke systemen. De AI Act en de AVG vullen elkaar aan.
- De AI Act en de AVG werken met verschillende categorieën onder hun persoonlijke werkingsfeer (aanbieder-gebruiker en verwerkingsverantwoordelijke-verwerker, afzonderlijk gedefinieerd in hun teksten). Onder welke categorie een notariële organisatie/notaris die een AI-systeem ontwikkelt/gebruikt, valt moet per geval worden bepaald.
- De rechtsgronden voor de verwerking van persoonsgegevens in verschillende notariële procedures zijn al vastgesteld. AI-oplossingen in deze procedures dienen alleen als hulp voor de notaris. Daarom is er voor de inzet van AI-systemen in principe geen wijziging nodig van de toegepaste rechtsgrond voor de verwerking van gegevens.
- De verwerking van speciale categorieën van persoonsgegevens ('*gevoelige gegevens*') kan aanwezig zijn bij het gebruik van gezichtsherkenning of systemen voor emotieherkenning en sentimentanalyse om de notaris te helpen. De AVG kwalificeert de verwerking van biometrische gegevens met als doel de unieke identificatie van een natuurlijke persoon onder de speciale categorie, wat een standaardverbod op dergelijke verwerking inhoudt. In tegenstelling tot de AI Act maakt de AVG geen onderscheid tussen de identificatie en verificatie van natuurlijke personen, en het verbod om biometrische gegevens te verwerken voor de verificatie is ook van toepassing, met als gevolg dat het alleen kan worden opgeheven met de uitdrukkelijke toestemming van de cliënt.
- Het gebruik van AI-systemen voor emotieherkenning en sentimentanalyse mag niet worden verboden betreffende het vorige punt, en de rechtsgronden voor verwerking met betrekking tot de procedure waarin dergelijke systemen worden ingezet, kunnen dezelfde blijven.
- Gebaseerd op de principes van transparantie, integriteit en vertrouwelijkheid wordt voorgesteld om af te zien van het gebruik van 'kant-en-klare' oplossingen in notariële procedures. Als de notaris toch gebruik wil maken van dergelijke AI-systemen is het sterk aan te raden om de persoonsgegevens van de betrokkenen te anonimiseren (zie details hieronder) in de prompt die aan het AI-systeem gegeven wordt, zodat de betrokkene later niet meer kan worden geïdentificeerd.
- Bij 'kant-en-klare' AI-oplossingen is het recht op gegevenswissing ('*recht om vergeten te worden*') extreem moeilijk of onmogelijk uit te oefenen, omdat dit betekent dat het vaak complexe systeem opnieuw getraind moet worden.
- Het verbod van de AVG op geautomatiseerde besluitvorming is waarschijnlijk niet van toepassing op het notariaat. De notaris moet altijd de eindbeslisser blijven; er wordt dus niet voldaan aan het criterium van het verbod van '*de beslissing uitsluitend gebaseerd op geautomatiseerde verwerking*'.
- Bij de ontwikkeling van notariële AI-systemen moet de ontwikkelaar er rekening mee houden dat het doel van de gegevensverwerking in individuele notariële zaken zich niet uitstrekt tot de daaropvolgende training van speciale AI-systemen. Er is een groot risico op verdere verwerking op een manier die niet overeenkomt met het oorspronkelijke doel. Bovendien kan het vinden van de juiste rechtsgrond voor een dergelijke verwerking (training van het AI-systeem) problematisch zijn.
- Dit betekent dat AI-systemen voor notarieel gebruik kunnen worden ontwikkeld met trainingsdata waarin de persoonsgegevens hele-

maal niet aanwezig of geanonimiseerd zijn, of waarbij de persoonsgegevens van bestaande betrokkenen worden vervangen door synthetische gegevens.

- De AVG-regels zijn niet van toepassing in geval van verwerking van geanonimiseerde gegevens. Bij gebruik van 'kant-en-klare' AI-oplossingen wordt het gebruik van geanonimiseerde gegevens sterk aanbevolen. Voor AI-training binnen het notariaat is het gebruik van synthetische gegevens een veilige optie.
- De verwerking van persoonsgegevens van overleden personen valt niet onder het

AVG-toepassingsgebied, maar er kunnen nationale regels gelden voor bescherming van dergelijke gegevens, waarmee rekening moet worden gehouden bij de ontwikkeling van AI.

- Soms kan het uitvoeren van een effectbeoordeling van fundamentele rechten en/of gegevensbeschermingseffectbeoordeling nodig zijn.
- In geval van twijfel over een van de vragen over AI en gegevensbescherming, wordt aangeraden de bevoegde gegevensbeschermingsautoriteiten te raadplegen voordat de betreffende activiteit begint.

VII. Bescherming van vertrouwelijke gegevens

1. Vertrouwelijke gegevens in notariële activiteiten

Notarissen in Europa zijn vertrouwde derden, wat in principe betekent dat ze een (wettelijke en/of deontologische) geheimhoudingsplicht hebben. Het beroepsgeheim heeft betrekking op de verplichting tot geheimhouding van de gegevens en informatie die door de cliënten worden verstrekt en andere relevante gegevens waarvan de notaris in het kader van zijn/haar beroepsactiviteit kennis neemt. Het beroepsgeheim van notarissen wordt echter uitsluitend geregeld door de toepasselijke nationale wetgeving, wat kan leiden tot grote verschillen tussen de Europese notariaten in verschillende landen. Bovendien kunnen er, zelfs als in een bepaald land het notariële beroepsgeheim is geregeld, situaties zijn waarin deze verplichting wordt opgeheven (bijvoorbeeld in het geval van strafrechtelijke vervolging). Dit hoofdstuk biedt een leidraad door uit te gaan van het principe dat het beroepsgeheim van toepassing is.

Notarissen verwerken dagelijks een enorme hoeveelheid gegevens die veel verder gaan dan alleen persoonsgegevens (het onderwerp van het vorige hoofdstuk). Dit kunnen ook openbaar beschikbare gegevens zijn, vertrouwelijke gegevens die bedrijfsgeheimen van cliënten kunnen bevatten en het kan ook niet worden uitgesloten dat staatsgeheimen of andere gekwalificeerde (bijv. militaire) geheimen voorkomen in notariële procedures (bijv. erfrechtprocedures) en diverse handelingen. Het doel van dit hoofdstuk is niet om een analyse te geven van de aard en behandeling van dergelijke gegevens in het algemeen. Dit hoofdstuk richt zich op het vermijden van risico's die voortvloeien uit het schenden van het beroepsgeheim bij het gebruik van AI-oplossingen. Anders dan andere fenomenen die alleen ingeperkt kunnen worden (bijv. AI-bias)—door op de juiste manier te werk te gaan—is het mogelijk om dergelijke risico's te vermijden.

2. Problemen met gegevensinvoer in AI-systemen

Zoals vermeld in verschillende hoofdstukken van dit Handboek, kunnen AI-oplossingen notarissen efficiënt ondersteunen bij hun werkzaamheden. Notarissen moeten

echter uiterst voorzichtig te werk gaan bij het kiezen van de oplossingen die ze voor verschillende doeleinden willen gebruiken. Zoals vermeld in het hoofdstuk waarin intern en extern ontwikkelde AI-systemen worden vergeleken, indien het notariaat een AI-systeem ontwikkelt, beschikt het over voldoende controle om er functionaliteiten in te bouwen die het behoud van het notariële geheim en de vertrouwelijkheid garanderen. Bij extern ontwikkelde systemen neemt het notariaat, als inkoper, in de individueel onderhandelde contractvoorwaarden bepalingen op die het technische behoud van het beroepsgeheim waarborgen.

Dit is echter heel anders en uitdagend in het geval van zogenaamde 'kant-en-klare' systemen, wat over het algemeen AI-systemen zijn die gratis beschikbaar zijn of tegen betaling op basis van de algemene voorwaarden van verschillende dienstverleners. Twee voorbeelden uit het dagelijks leven zijn ChatGPT om tekst te genereren en de toepassing DeepL voor automatische vertaling. De leveranciers van dergelijke diensten beloven vaak strikte vertrouwelijkheid van de gegevens die in het systeem worden ingevoerd (veel van hen alleen in het geval van betalende, geüpgradede versies). De verificatie hiervan blijft echter een probleem.

Allereerst geldt als algemene regel dat de algemene voorwaarden en condities van 'kant-en-klare' AI-systemen volledig ongelezen blijven, en de meerderheid van de gebruikers simpelweg alleen op de knop klikt om ze te accepteren. Dit is volkomen redelijk gedrag, omdat bij sommige activiteiten (bijv. het genereren van e-mails, eenvoudige vertalingen) het grondig lezen en interpreteren van dergelijke termen een buitensporige last zou vormen en tijdrovend is.

Ten tweede is het, vooral in het geval van LLM's en generatieve AI-systemen, zo dat het model over het algemeen 'leert' van de input (prompts) van de gebruikers. Zodra de gegevens in het systeem zitten blijven ze daar, want met de huidige technologie is het verwijderen van een deel van de dataset uit het systeem alleen mogelijk door het AI-model volledig opnieuw te trainen. Vanzelfsprekend is dat voor modellen zoals GPT-4 een onrealistische verwachting. Als vertrouwelijke gegevens worden ingevoerd in het gegeven AI-systeem blijven ze daar hoogstwaarschijnlijk opgesla-

gen en gebruikt het AI-algoritme ze voor het genereren van outputs. In het ergste geval kan de output van het systeem de vertrouwelijke gegevens bevatten die zijn geleerd van de prompt van de gebruiker en bestaat de mogelijkheid dat deze in handen komen van onbevoegden.

3. Oplossingen om schending van het beroepsgeheim te voorkomen

In het geval van intern ontwikkelde AI-oplossingen en systemen besteld bij externe leveranciers moeten de relevante kwesties al in de ontwerp- en ontwikkelingsfase van de gegeven oplossing worden geïdentificeerd en aangepakt. Dit vereist samenwerking tussen notarissen en ontwikkelaars om de behoeften en oplossingen te identificeren en te integreren die de bescherming van het beroepsgeheim garanderen.

Waar ‘kant-en-klare’ oplossingen worden gebruikt moeten notarissen uiterst voorzichtig te werk gaan en elke invoer vermijden die vertrouwelijke gegevens kan bevatten (sommige aanbieders bieden opties aan die—op basis van hun advertenties—verder geen gebruik maken van de invoergegevens, maar dit kan niet worden geverifieerd/is uiterst moeilijk te verifiëren). Het kan bijvoorbeeld een veilige optie zijn om gegevens handmatig te maskeren of te verwijderen uit de prompts en de oorspronkelijke gegevens opnieuw te verwerken bij het controleren van de output (wat altijd nodig is om de juistheid van het document te garanderen – zie het Hoofdstuk over ‘Human-in-the-loop’).

Als dit niet kan worden uitgevoerd, wordt notarissen sterk aangeraden het betreffende systeem niet te gebruiken en, als er geen andere geschikte oplossing beschikbaar is, de betreffende taak uit te voeren zonder het gebruik van AI.

Belangrijkste conclusies

- Notarissen in Europa zijn vertrouwde derden en zijn gebonden aan de plicht van professionele zorgvuldigheid, waarvan de precieze regels worden bepaald door nationale wetten.
- Notarissen verwerken een enorme hoeveelheid gegevens, waaronder persoonsgegevens, openbare gegevens en vertrouwelijke gegevens.
- Door op de juiste manier te werk te gaan is het absoluut mogelijk om schending van het beroepsgeheim te vermijden.
- Als het notariaat een AI-systeem ontwikkelt, heeft het voldoende controle om er functies in te bouwen die het behoud van het notariële geheim waarborgen.
- Bij extern ontwikkelde systemen neemt het notariaat, als inkoper, in de individueel onderhandelde contractvoorwaarden bepalingen op die het technische behoud van het beroepsgeheim waarborgen.
- Bij gebruik van kant-en-klare systemen kan, ondanks de beloften van hun aanbieders, de bescherming van het beroepsgeheim niet aantoonbaar worden gegarandeerd.
- 'Kant-en-klare LLM's en generatieve AI-systemen 'leren' van de prompts van de gebruiker, inclusief de gegevens die door het beroepsgeheim moeten worden beschermd.
- Als 'kant-en-klare' oplossingen worden gebruikt, moeten de relevante gegevens worden gemaskeerd of weggelaten uit de prompts. Als dit niet mogelijk is, mag de notaris het betreffende systeem niet gebruiken.

VIII. AI-bias en -hallucinatie

1. Oorzaken en gevolgen van AI-bias

In de hele Europese Unie (en ook daarbuiten) zijn de principes en verplichtingen van onpartijdigheid en neutraliteit kenmerkend voor het notariaat. Als hier niet efficiënt mee wordt omgegaan kunnen ze in gevaar komen door het gebruik van AI-oplossingen, wat een negatieve invloed kan hebben op de betrouwbaarheid van de hele beroepsgroep.

Strikt genomen is AI-bias een afwijking in de output van het AI-systeem die twee belangrijke bronnen heeft:

- vooroordelen in de trainingsdata en/of
- vooringenomen aannames tijdens de ontwikkeling van het AI-algoritme.

Beide bronnen zijn echter terug te voeren op de inherente kenmerken van de menselijke geest, die van nature wordt gekenmerkt door bias. AI-systemen worden gemaakt door mensen die duidelijk hun individuele of groepsbias weerspiegelen (bijv. de bias van de AI-programmeurs). Bias is meestal niet opzettelijk en kan niet worden gedetecteerd voordat het AI-systeem in gebruik wordt genomen.

Bias in het AI-systeem resulteert mogelijk in discriminatie en leidt tot de schending van het eerlijkeheidsbeginsel door onjuiste aanbevelingen te geven en oneerlijke beslissingen voor te stellen.

Historische onevenwichtigheden en maatschappelijke vooroordelen worden zeer waarschijnlijk weerspiegeld in de trainingsdata. Bias kan ontstaan in verschillende stadia van gegevensverzameling en verwerking en kan van verschillende aard zijn.

Steekproefbias treedt op wanneer de verzamelde gegevens niet representatief zijn voor het te analyseren doel. Deze onevenwichtige gegevens resulteren in AI-bias in de richting van de categorie met de grootste hoeveelheid data. Meetvertekening ontstaat door fouten in gegevensverwerking wanneer de verzamelde gegevens niet nauwkeurig worden gemeten. Uitsluitingsbias treedt op wanneer gegevens ten onrechte worden weggelaten uit de trainingsdataset en confirmatiebias treedt op wanneer de

verwachtingen van de datacleaner invloed hebben op het reinigingsproces.

Een speciaal soort bias is een selectiebias dat bekend staat als 'overlevingsbias', wat ernstige gevolgen kan hebben voor de ontwikkeling en ook voor de inzet van AI-systemen. Overlevingsbias negeert de onsuccesvolle uitkomsten in een selectieproces. Dit betekent dat bij het maken van de selectie van een specifieke groep of dataset, de focus alleen ligt op voorbeelden van succesvolle elementen ('overlevers', bijv. winstgevendende transacties, bedrijven met hoge winsten) en niet op de groep of dataset als geheel (inclusief de mislukte transacties en minder goed functionerende bedrijven). Dit leidt tot onvolledige gegevens en heel vaak tot onjuiste output.

Ook in AI-gegevensverzameling leidt overlevingsbias tot de selectie van trainingsdata die vooral succesvolle voorbeelden vertegenwoordigen (bijv. transacties waarbij de schuldenaar zijn/haar plichten vervulde) en tot uitsluiting van mislukte of onsuccesvolle voorbeelden (bijv. transacties waarbij gerechtelijke vervolging wegens wanprestatie plaatsvond). Dit kan leiden tot een beperking van de verscheidenheid aan outputs die door het AI-systeem gegenereerd worden en tot het missen van inzichten en kansen voor verbetering.

Overlevingsbias kan de ontwikkeling en evaluatie van AI-modellen aanzienlijk beïnvloeden. Bij het selecteren van het AI-model kan de aanwezigheid van overlevingsbias ertoe leiden dat de voorkeur wordt gegeven aan bekende AI-algoritmen van grote multinationale bedrijven, waardoor alternatieve oplossingen die mogelijk nauwkeuriger en geschikter zijn voor de betreffende taken over het hoofd worden gezien. Bovendien kan overlevingsbias de evaluatie van AI-algoritmen beïnvloeden en leiden tot een overschatting van de prestaties van sommige oplossingen, omdat de aandacht uitsluitend uitgaat naar de succesvolle uitkomsten en de negatieve uitkomsten over het hoofd worden gezien.

2. Identificatie en beperking van bias (de-biasing)

Als AI-systemen complexer worden en getraind worden op steeds meer gegevens, zal het identificeren en beperken van bias steeds moeilijker worden.

Gebaseerd op de bovenstaande verklaringen is het volledig verwijderen van bias uit de AI-systemen niet mogelijk, maar het zo veel mogelijk beperken en verminderen van vooringenomen outputs kan wel een realistisch doel zijn. Desondanks moet worden toegegeven en geaccepteerd dat zelfs een betrouwbaar AI-model nog steeds bias bevat omdat bias inherent is aan ML. Het is ook precies om deze reden dat de tussenkomst van de notaris vereist is, ook wanneer de notaris gebruik maakt van AI-systemen.

In de eerste plaats moet het doel van het AI-model duidelijk worden gedefinieerd. Dit houdt in dat objectieve regels voor het in- en uitsluiten van gegevens moeten worden bepaald om in de fase van gegevensopschoning al een uitgebalanceerde dataset te hebben. In de ontwikkelingsfase kan de documentatie van de gegevensverzameling en verwerkingsactiviteiten zeer nuttig zijn om transparantie te bieden voor het identificeren van de delen of items van de dataset die de bias van het AI-systeem veroorzaakt. Het is nuttig om dit ook uit te voeren als de relevante dataset verandert. Dit kan ook effectief worden toegepast op het AI-algoritme om potentiële problemen met bias te vinden en corrigerende maatregelen te nemen.

Om het probleem van bias zo efficiënt mogelijk aan te pakken moeten trainingsdata en het toegepaste algoritme regelmatig en nauwkeurig worden gecontroleerd en uitgebreid worden geaudit. Na detectie van afwijkingen moet de trainingsdataset worden uitgebreid en/of gewijzigd en/of moet het algoritme worden aangepast.

Net als met andere vormen van bias kan overlevingsbias alleen worden beperkt en niet volledig worden vermeden. Het belangrijkste is dat er gegevens worden opgenomen in de trainingsdataset die ook negatieve uitkomsten vertegenwoordigen. Bovendien kunnen een objectievere en uitgebreidere evaluatie van het in te zetten AI-algoritme en—bij het gebruik van extern aangeleverde algoritmen—het overwegen van het gebruik van algoritmen die niet alleen door bekende bedrijven worden aangeleverd, overlevingsbias helpen verminderen. Door deze feedback kan de dataset en het algoritme effectief worden verfijnd.

In eenvoudige gevallen kan het systeem intern worden uitgevoerd, maar er zijn al verschillende academische en marktgebaseerde oplossingen voor dit proces beschikbaar, waarvan er vele open-source zijn. Een dergelijke oplossing is bijvoorbeeld AI Fairness 360, die helpt bij het identificeren en beperken van bias.

De menselijke rol in het 'de-biasing' van AI-oplossingen voor notarissen is cruciaal, en deze taak moet niet worden uitgevoerd door IT-experts alleen, maar in samenwerking met notarissen die op basis van hun kennis en ervaring het best in staat zijn om de meest voorkomende situaties te herkennen waarin bias kan optreden.

Na het verkrijgen van output van het AI-systeem moeten notarissen deze ook zorgvuldig controleren op het vinden van bias. Vooringenomen output moet in de specifieke gevallen buiten beschouwing worden gelaten voor de notariële activiteit en de bevoegde ontwikkelaar moet op de hoogte worden gesteld van het probleem om het te beperken.

3. Oorzaken en effecten van AI-hallucinaties

AI-hallucinaties—wat nauw verwant is aan de kwestie van bias—wordt vaak genoemd en kan een aanzienlijke invloed hebben op het gebruik van AI-systemen binnen het notariaat. Het fenomeen van AI-hallucinaties komt voor bij LLM's, meestal tijdens het gebruik van generatieve AI-oplossingen, en bestaat uit het leveren van output die niet bestaat (dus onjuist is). Daarbij toont een 'hallucinerende' AI in zijn output 'een hoge mate van vertrouwen' met betrekking tot de nauwkeurigheid ervan. Dit staat sterk in contrast met de standaardverwachtingen van de menselijke gebruikers, die op zoek zijn naar de meest geschikte en precieze output voor hun prompts aan het AI-systeem (net zoals we in het echte leven correcte antwoorden op onze vragen verwachten van onze dienstverleners).

Het meest beruchte geval van AI-hallucinaties uit de juridische wereld komt uit de Verenigde Staten, waar een advocaat, Steven A. Schwartz, documenten naar de rechtbank stuurde met daarin allerlei niet-bestaande jurisprudentie. De advocaat gebruikte ChatGPT om hem te helpen bij het opstellen van de documenten, en het systeem verzong zaken die volledig en overtuigend echt leken. De advocaat ging onzorgvuldig te werk door de zaken die door het systeem werden aangeleverd niet te verifiëren. Ze werden echter door de bevoegde rechter als niet-bestaand

bestempeld, wat leidde tot aansprakelijkheid en reputatieschade voor de advocaat.

De tweede bron van AI-hallucinatie is de complexiteit van het model. De technologische basis van LLM's is een specifiek neurale netwerk waarvan de besluitvormingsprocessen moeilijk te begrijpen zijn (LLM's zijn 'niet-deterministisch'). Hallucinatie kan optreden door overfitting van het AI-model, oftewel: wanneer het model te veel getraind is op zijn trainingsdata (inclusief de 'ruis', die voor het betreffende doel irrelevante gegevenselementen zijn) in plaats van het leren van de onderliggende patronen. Dit heeft tot gevolg dat de LLM onnauwkeurige output genereert omdat het de trainingsdata heeft geleerd, maar niet de onderliggende patronen.

De derde bron is het gebrek aan contextueel begrip (d.w.z. de omgang met de context), wat ertoe leidt dat AI-modellen moeite hebben met contextspecifieke problemen. Dit kan leiden tot de situatie waarin een model een grammaticaal accurate maar verder betekenisloze output genereert.

4. Beperken van AI-hallucinatie

De verklaringen van AI-hallucinatie in het vorige punt veranderen niets aan het feit dat het fenomeen van hallucinatie de indruk wekt dat deze systemen onbetrouwbaar zijn, en het vertrouwen van hun gebruikers aanzienlijk kan worden geschonden. Dit kan vooral problematisch zijn in het geval van beroepen zoals het notariaat, waar belangrijke beslissingen worden genomen waarbij de nauwkeurigheid van gegevens en informatie cruciaal is en het gebrek hieraan kan leiden tot ernstige negatieve gevolgen. Een AI-tool voor antiwitwasdoeleinden die hallucineert, kan bijvoorbeeld vals positieven geven (iets als verdacht markeren terwijl het dat in feite niet is) of vals negatieven (iets als niet-verdacht identificeren terwijl het dat wel is).

Tegelijkertijd kan het nauwkeurige gebruik van betrouwbare AI-systemen het beroep veel voordelen opleveren en zou het betreuwenswaardig zijn om het gebruik van dergelijke systemen volledig af te schaffen als gevolg van enkele negatieve ervaringen. Daarom zijn er ook verschillende oplossingen om AI-hallucinatie te beperken.

Allereerst is het noodzakelijk om ervoor te zorgen dat het toegepaste AI-model is getraind met een kwalitatieve (volledig, relevant, consistent) dataset, en dat er voldoende

de contextuele en verschillende gegevens worden gebruikt tijdens het trainingsproces om de problemen van overfitting te voorkomen.

Ten tweede—vooral in het begin van de implementatie—kan het programmeren van het AI-model om zijn output te genereren op basis van vooraf bepaalde sjablonen, en het stellen van grenzen aan de mogelijke uitkomsten, bijdragen aan de nauwkeurigheid van de output.

Ten derde moeten de ingezette AI-modellen regelmatig worden gecontroleerd aan de hand van bekende informatie uit de echte wereld die de context weerspiegelt, en op basis van deze controles moeten ze waar nodig worden aangepast of opnieuw worden getraind.

In deze context moet het proces van 'AI grounding' kort worden genoemd, aangezien o.a. het probleem van hallucinatie kan worden aangepakt door het AI-systeem (meestal de LLM's, vooral NLP oplossingen) te gronden/aarden in de echte wereld. Specifiek betekent grounding het proces van het koppelen van AI-outputs aan contexten en kennis uit de echte wereld. Zonder dit proces zijn AI-modellen beperkt tot hun initiële trainingsdata en het tijdsbestek van die gegevens, en genereren ze output die niet overeenkomt met de werkelijkheid, wat leidt tot onjuiste conclusies. Grounding kan meestal worden bereikt door domeinspecifieke data (externe gegevensbronnen) te integreren en de trainingsdataset van de AI voortdurend bij te werken (met real-time gegevens die nieuwe omstandigheden weerspiegelen). De voordelen van grounding zijn onder andere de grotere nauwkeurigheid, relevantie en betrouwbaarheid van de AI-output. Grounding is echter een complexe taak van zowel technologische als menselijke kant (domeinexperts).

Tot slot is ook hier de rol van menselijke (notariële) controle van de output cruciaal. De notaris moet zorgvuldig de nauwkeurigheid van de gegeven output verifiëren, of het nu gaat om een verwijzing naar een wettelijke bepaling, jurisprudentie of informatie die is afgeleid van gegevens uit de praktijk (bijv. de combinatie van gegevens uit registers of documenten). Door het tijdig opsporen en signaleren van hallucinatie (feedback van de gebruiker) kunnen notarissen bijdragen aan de verbetering van het betreffende AI-systeem.

Idealiter geeft de combinatie van deze oplossingen het best mogelijke resultaat. Dit vereist een nauwe samenwerking tussen notarissen en IT-specialisten.

Belangrijkste conclusies

- AI-bias is een afwijking in de uitvoer door het AI-model met twee belangrijke bronnen: de vooroordelen in de trainingsdata en/of de vooringenomen aannames die zijn gedaan tijdens de ontwikkeling van het AI-algoritme.
- De reden van AI bias is dat AI-systemen worden gemaakt door mensen en hun—meestal onbedoelde maar natuurlijke—vooroordelen weerspiegelen.
- Bias in het AI-systeem resulteert mogelijk in discriminatie en leidt tot de schending van het eerlijkeheidsbeginsel.
- Overlevingsbias is een speciaal type bias dat gekenmerkt wordt door het negeren van de niet-succesvolle uitkomsten in een selectie-proces, wat leidt tot de onvolledigheid van gegevens en heel vaak tot onjuiste uitkomsten.
- Het volledig uitsluiten van bias uit AI-systemen is over het algemeen niet mogelijk. Alleen het beperken van bias is realistisch.
- Om het probleem van bias zo efficiënt mogelijk aan te pakken moeten trainingsdata en het toegepaste algoritme regelmatig en nauwkeurig worden gecontroleerd en uitgebreid worden geaudit.
- Notarissen moeten AI-output zorgvuldig controleren op bias. Vooringenomen output moet buiten beschouwing worden gelaten voor de notariële activiteit.
- Het fenomeen van AI-hallucinatie komt onder andere voor bij Large Language Models (LLM's), meestal in generatieve AI-oplossingen.
- De hallucinerende AI geeft 'met een hoge mate van betrouwbaarheid' output die niet bestaat.
- AI-hallucinatie kan meestal worden teruggevoerd op de onderliggende technologie zelf.
- Om hallucinatie te beperken moet de trainings-dataset van hoge kwaliteit zijn en voldoende contextuele en diverse gegevens bevatten.
- Menselijk toezicht en feedback zijn cruciaal voor het detecteren en beperken van hallucinatie.

IX. Transparantie en verklaarbaarheid van AI-systemen

1. Algemene inzichten

Inzicht in de werking van de AI-systemen en de mogelijkheden en beperkingen ervan is cruciaal om verkeerd gebruik van deze systemen te voorkomen en om de risico's van de inzet van AI te vermijden of te beperken. AI-aanbieders hebben de inherente ethische en—binnen de EU als gevolg van de AI Act—wettelijke verplichting om de transparantie van hun systemen te waarborgen, wat onder meer inhoudt dat zij informatie moeten verstrekken over wat het systeem dat ze hebben ontwikkeld kan doen, voor welke toepassingen het geschikt en ongeschikt is, en volgens welke regels en methoden de AI tot een output komt.

Het juiste niveau van transparantie en verklaarbaarheid draagt op efficiënte wijze bij aan het juiste en efficiënte gebruik van de AI-modellen door de aanbieders die werken aan AI-oplossingen op basis van het geleverde model, evenals aan de eindgebruikers (gebruikers) van dergelijke systemen. Bovendien vergroten transparantie en verklaarbaarheid het algemene vertrouwen van de gebruiker en de samenleving in AI-oplossingen, wat cruciaal is in de huidige tijd waarin deze technologie wordt omgeven door scepsis. Ten slotte helpen transparantie en verklaarbaarheid bij het naleven van de relevante regelgeving.

2. AI-transparantie en -verklaarbaarheid – de belangrijkste verschillen

Hoewel ze nauw met elkaar verbonden zijn, zijn er belangrijke verschillen tussen de termen 'transparantie' en 'verklaarbaarheid' die verschillende benaderingen en methoden vereisen van de aanbieders en van de gebruikers van het betreffende AI-systeem. Zowel transparantie als verklaarbaarheid zijn erop gericht AI-systemen begrijpelijk, regelgevingsconform en betrouwbaar te maken, maar op verschillende manieren.

AI-transparantie richt zich op het 'hoe'. Preciezer gezegd betekent het de toegankelijkheid van informatie voor de personen met bevoegdheden en rechten (bijv. autoriteiten, gebruikers, betrokken personen) over hoe een AI-systeem

is ontwikkeld en hoe het functioneert (oftewel 'wat er achter de schermen gebeurt'). Dit moet de hele levenscyclus van het betreffende AI-systeem omvatten, inclusief informatie over de data gebruikt om het systeem te trainen, de gebruikte algoritmen, en de belangrijkste details van de ontwikkeling en implementatie.

AI-verklaarbaarheid richt zich op het geven van duidelijke en begrijpelijke redenen voor specifieke AI-resultaten (bijv. voorspellingen, beslissingen, aanbevelingen), zodat het duidelijk is waarom deze resultaten zijn geleverd. In het geval van aanbevelingen voor het oplossen van een rechtszaak moet de jurist bijvoorbeeld beschikken over de relevante gegevens en informatie waarop de specifieke aanbeveling is gebaseerd. Dit zorgt ervoor dat de gebruiker van het AI-systeem de nauwkeurigheid van de output kan verifiëren en garanderen dat de uiteindelijke menselijke beslissing gebaseerd zal zijn op gefundeerde AI-ondersteunde informatie. Op deze manier kan de gebruiker het benodigde niveau van vertrouwen hebben in de specifieke output van het systeem.

Samengevat: verklaarbaarheid richt zich op het begrijpelijk maken van individuele output, transparantie zorgt voor duidelijkheid over de werking van het AI-systeem.

Bovendien maakt de wetenschap het onderscheid tussen de volgende drie transparantieniveaus: algoritmische transparantie, interactietransparantie en sociale transparantie. Zonder diep op de inhoud van deze termen in te gaan, richt algoritmische transparantie zich op de interne werking van het algoritme en wat hierboven is beschreven onder 'AI-transparantie'. Interactietransparantie omvat de interacties tussen mens en machine, oftewel gebruikers en AI-systemen, is meer gerelateerd aan wat hierboven is beschreven onder 'AI-verklaarbaarheid', en richt zich op de begrijpelijkheid van dergelijke interacties, en de begrijpelijkheid van wat gebruikers kunnen verwachten van hun interacties met de AI. Ten slotte richt sociale transparantie zich op de bredere impact van AI-systemen op de samenleving, inclusief ethiek, eerlijkheid en rechtvaardigheid, bias en privacy.

3. Methoden voor transparantie en verklaarbaarheid

Transparantie kan worden bereikt door nauwkeurige en uitgebreide documentatie en openbaarmaking van de belangrijkste aspecten van het betreffende AI-systeem. Voor AI-systemen met een hoog risico die als zodanig worden gekwalificeerd door de AI Act is er bijvoorbeeld een lijst van documenten en informatie die bij het AI-systeem aanwezig moeten zijn. In gevallen waarin meer of andere informatie over het systeem verplicht is vanwege speciale nalevingsverplichtingen of simpelweg vanwege de individuele eisen van de betreffende gebruiker moet er andere informatie en documentatie worden toegevoegd aan het aangeboden AI-systeem. De documentatie bevat onder andere de gegevensbronnen en de belangrijkste bewerkingen die zijn uitgevoerd op de trainingsdata, de beschrijving van de toegepaste algoritmen en hun processen. Om transparant te zijn moet de documentatie het doel en de beperkingen van het AI-systeem en de potentiële bias omschrijven. Dit laatste kan effectief worden beperkt door de relevante documentatie te gebruiken, specifiek door de gegevens en/of de eigenschap van het algoritme te vinden die de bias veroorzaken.

AI-verklaarbaarheid kan worden verkregen door middel van verschillende technieken om de output van AI-systemen begrijpelijk te maken voor gebruikers. Er zijn enkele technologische methoden uitgewerkt die complexe modellen uiteenzetten en identificeren hoe verschillende gegevens en algoritme-eigenschappen bijdragen aan een specifieke output.

4. Transparantieverplichtingen in de AI Act

In overweging 27 van AI Act maakt de wetgever niet het bovenstaande scherpe onderscheid tussen transparantie en verklaarbaarheid, maar voegt ze samen: *“transparantie betekent dat AI-systemen worden ontwikkeld en gebruikt op een manier die passende traceerbaarheid en verklaarbaarheid mogelijk maakt, terwijl mensen zich ervan bewust zijn dat ze communiceren of te maken hebben met een AI-systeem en gebruikers naar behoren worden geïnformeerd van de mogelijkheden en beperkingen van dat AI-systeem en de betrokken personen over hun rechten”*.

De AI Act introduceert 3 niveaus van transparantieverplichtingen: de algemene regels zijn van toepassing op alle relevante AI-systemen, AI-systemen met een hoog risico

vallen onder strengere transparantieverplichtingen en de aanbieders van AI-modellen voor algemene doeleinden hebben de strengste en meest uitgebreide verplichtingen.

Artikel 50 van de AI Act voert een algemene transparantieregeling in voor elk AI-systeem als het onder een van de genoemde gevallen valt. Aanbieders moeten er bijvoorbeeld voor zorgen dat AI-systemen die bedoeld zijn voor rechtstreekse interactie met natuurlijke personen zodanig worden ontworpen en ontwikkeld dat de betrokken natuurlijke personen ervan op de hoogte zijn dat zij te maken hebben met een AI-systeem indien dit voor de betrokken personen niet direct duidelijk is. Deze verplichting geldt onder andere voor chatbots en moet uiterlijk bij de eerste interactie met of blootstelling aan het AI-systeem door individuen plaatsvinden.

Artikel 13 van de AI Act bevat transparantieverplichtingen voor aanbieders van systemen met een hoog risico in algemene zin. Dit houdt in dat de relevante aanbieders hun systemen zodanig moeten ontwerpen en ontwikkelen dat er voldoende transparantie is voor gebruikers om de werking en output van het systeem redelijkerwijs te begrijpen. Bovendien moeten ze *‘gebruiksaanwijzingen’* geven aan gebruikers die duidelijke en volledige informatie geven over de kenmerken, werking en andere belangrijke kenmerken van het AI-systeem met een hoog risico.

Tot slot, volgens artikel 53 van de AI Act, moeten aanbieders van AI-modellen voor algemene doeleinden voldoen aan specifieke transparantieverplichtingen vanwege de complexe kenmerken en mogelijkheden van dergelijke modellen, waardoor het nog moeilijker wordt om de werking ervan te begrijpen. Dergelijke aanbieders creëren relevante technische documentatie over hun training, test- en evaluatieprocessen, en verstrekken informatie en documentatie aan aanbieders van AI-systemen die het model willen gebruiken in hun producten, om de mogelijkheden en beperkingen van het model te begrijpen en een gedetailleerd overzicht te geven van de trainingsinhoud en -data.

5. Black box AI vs. white box AI

Vooral in het geval van large language models blijft het zogenaamde *‘black box-probleem’* een belangrijk obstakel voor zowel de transparantie als de verklaarbaarheid van AI.

De maatschappelijke behoefte aan transparante en verklaarbare AI blijkt uit een recente ontwikkeling van

het bedrijf OpenAI (ontwikkelaar van ChatGPT), dat een AI-model lanceerde met de naam o1. Dit is een AI-oplossing met redeneercapaciteiten, die zichtbaar 'hardop denkt' over waarom het doet wat het doet, met de bedoeling om menselijke gebruikers te laten begrijpen welke stappen het AI-model neemt om tot een conclusie te komen. De details van wat de AI echt doet blijven echter onder de motorkap omwille van de bescherming van bedrijfsgeheimen, en deze situatie zal waarschijnlijk ongewijzigd blijven.

In de klassieke situatie waarin de gebruiker wordt geconfronteerd met het black box-probleem—door de ondoorzichtigheid van het AI-algoritme, kent hij/zij de input en de output, maar kan hij/zij niet begrijpen waarom het gegeven AI-systeem tot een bepaalde conclusie is gekomen (wat is er gebeurd tussen de invoer en de uitvoer van het systeem?). Bovendien is het bij zelflerende algoritmen heel vaak zo dat zelfs de ontwikkelaars van de betreffende AI-oplossing—ondanks hun hoge niveau van IT-kennis—niet in staat zijn om te begrijpen en uit te leggen hoe de gegeven output tot stand is gekomen. Het black box-fenomeen betekent niet noodzakelijk dat de output van dergelijke systemen onjuist is. Integendeel: dankzij hun complexiteit kunnen ze extreem nauwkeurige outputs leveren. Het probleem is het gebrek aan inherent vertrouwen in dergelijke AI-oplossingen vanwege het gebrek aan transparantie en verklaarbaarheid.

Daarentegen is de zogeheten 'white box AI' transparant over hoe het tot zijn conclusies komt: de werking van het algoritme en de factoren die de output beïnvloeden kunnen worden gevolgd en begrepen door de gebruikers. Dit resulteert in meer vertrouwen van de kant van gebruikers, zelfs als deze modellen beperktere mogelijkheden hebben.

Black box AI kan ongeschikt zijn voor sterk gereguleerde sectoren, zoals het notariaat, maar kan nog steeds ongelooflijk nuttig zijn voor andere industrieën of sectoren.

6. Het belang van AI-transparantie en -verklaarbaarheid in het notariaat

In verschillende sectoren hebben de betrokken beroepsgroepen niet alleen de plicht om te begrijpen hoe de gebruikte technologische oplossingen werken, maar ook om hun werking uit te leggen aan klanten. Over het algemeen geven notarissen cliënten juridisch advies, stellen ze akten op, nemen ze bindende niet-contentieuze beslissingen en hebben ze de plicht om de rechtsgrondslag van

deze activiteiten en de juridische gevolgen ervan op een begrijpelijke manier uit te leggen. De algemene plicht om cliënten te informeren over de toegepaste technologische oplossingen, over hun werking en hun diepgang is sterk afhankelijk van de bepalingen van de nationale wetgeving die van toepassing is op het betreffende notariaat.

Overeenkomstig artikel 26, lid 11, van de AI Act: *'gebruikers van AI-systemen met een hoog risico bedoeld in bijlage III die beslissingen nemen of assistentie verlenen bij het nemen van beslissingen met betrekking tot natuurlijke personen, stellen de natuurlijke personen ervan in kennis dat zij onderworpen zijn aan het gebruik van het AI-systeem met een hoog risico'*. Deze verplichting om cliënten te informeren geldt alleen als de betreffende instelling een specifiek AI-systeem met een hoog risico gebruikt (de AI-systemen meteen hoog risico die mogelijk worden gebruikt door het notariaat worden geanalyseerd in een apart hoofdstuk van dit handboek) dat de notaris helpt bij het nemen van een beslissing. Dit kan vooral gebeuren bij niet-contentieuze notariële procedures. Andere beslissingen van de notaris, bijvoorbeeld het weigeren om verder te gaan op basis van een emotieherkenningsysteem met een hoog risico, kan ook de verplichting van de notaris om de cliënten te informeren in werking stellen. Volgens overweging 93 *'moet zijn informatie het beoogde doel en het soort beslissingen dat het neemt, omvatten.'* De gebruiker moet de natuurlijke personen ook informeren over hun recht op een verklaring die krachtens deze verordening wordt verstrekt.' Daarom is dit geen verplichting om de werking van het gegeven systeem uit te leggen.

Het eerder genoemde recht op uitleg is te vinden in artikel 86 van de AI Act: *'Elke betrokken persoon die onderworpen is aan een beslissing die door de gebruiker op basis van de output van een AI-systeem met een hoog risico genoemd in bijlage III, met uitzondering van de in punt 2 van die bijlage genoemde systemen, en die rechtsgevolgen heeft of op een vergelijkbare wijze significante gevolgen voor die persoon heeft op een wijze die hij als nadelig voor zijn gezondheid, veiligheid of grondrechten beschouwt, heeft het recht om van de gebruiker duidelijke en zinvolle uitleg te krijgen over de rol van het AI-systeem in de besluitvormingsprocedure en de belangrijkste elementen van de genomen beslissing.'*

Als de notaris dus bepaalde AI-systemen met een hoog risico genoemd in bijlage III toepast, een beslissing moet nemen en zijn/haar beslissing een van de bovengenoemde gevolgen heeft, gebaseerd is op de AI-output, dan heeft de getroffen persoon het recht om van de notaris uitleg te krijgen over het ingezette AI-systeem. Voor de toepassing van dit artikel moet tegelijkertijd aan verschillende voorwaarden worden voldaan: een specifiek systeem met een hoog risico moet worden gebruikt en de output van dat systeem moet de basis zijn van de beslissing van de notaris. Deze beslissingen hebben onvermijdelijk juridische of andere significante gevolgen voor een natuurlijke persoon. In notariële procedures, met uitzondering van enkele notariële niet-contentieuze procedures, is de kans klein dat de betreffende beslissing negatieve gevolgen heeft voor de grondrechten van een natuurlijke persoon. Niettemin is het belangrijk om in gedachten te houden dat artikel 86 van de AI Act de noodzaak benadrukt voor notarissen die AI-systemen met een hoog risico toepassen om de werking van dergelijke oplossingen te begrijpen en te allen tijde voorbereid te zijn op dergelijke verzoeken van hun cliënten en het gebruik ervan bekend te maken.

Bovendien moeten notarissen, met het oog op het behoud van het positieve imago van het beroep, bij een verzoek van hun cliënten over de werking van de gebruikte AI-oplossing, in staat zijn hun de nodige informatie te verstrekken, zelfs als er in een bepaald rechtsgebied geen uitdrukkelijke verplichting bestaat om cliënten proactief te informeren over de gebruikte technologie of als artikel 86 van de AI Act in de betreffende situatie niet van toepassing is.

In gevallen waarin het haalbaar is, kan het praktisch zijn voor notarissen die besluiten om gebruik te maken van AI-systemen met een hoog risico om een document te hebben met aan het einde een verklaring dat de notaris de cliënten heeft geïnformeerd dat hij/zij een AI-systeem met een hoog risico gebruikt. Deze verklaring wordt ondertekend door de cliënten als bewijs dat de notaris aan zijn verplichting heeft voldaan. Dit document kan ook een eenvoudige en begrijpelijke uitleg bevatten over hoe het systeem werkt.

Zoals gezegd is het gebruik van AI door notarissen geen doel op zich, maar is het een hulpmiddel om hun werk te stroomlijnen, te vergemakkelijken en hun efficiëntie te verhogen. Om de mogelijkheden van de AI ten volle te benutten, moeten notarissen een zekere mate van vertrouwen hebben in deze oplossingen wanneer ze beslis-

singen nemen over het gebruik ervan, vooral wanneer er veel op het spel staat. Daarom speelt AI-transparantie en -verklaarbaarheid ook voor notarissen een cruciale rol. Het is belangrijk om ook hier te benadrukken dat de notaris in alle gevallen de eindbeslisser moet zijn. Hij/zij moet dus in staat zijn om beslissingen, aanbevelingen of andere output van het AI-systeem te omzeilen wanneer het niet voor hem/haar niet volledig te begrijpen is waarop die output is gebaseerd. Hieronder vallen ook situaties die ontstaan door het ontbreken van transparantie en/of verklaarbaarheid.

Als de ontwikkelaar van de betreffende AI-oplossing de notariële organisatie is waar de notaris lid van is, moet de organisatie de transparantie en verklaarbaarheid garanderen door alle nodige informatie te verstrekken over het AI-systeem en de notaris permanent bij te staan als daarover vragen opkomen. Tegelijkertijd zouden notarissen de ontwikkelaar moeten voorzien van feedback en inzichtelijke informatie uit hun praktijk en ervaring om onder andere de transparantie en verklaarbaarheid van het systeem te vergroten. Afhankelijk van de classificatie van het intern ontwikkelde AI-systeem of model op basis van de AI Act (hoog risico, laag risico, geen risico of algemene doeleinden), moet de aanbieder (de organisatie) de toepasselijke transparantie- en verklaarbaarheidsverplichtingen in acht nemen en naleven.

Als het AI-systeem is ontwikkeld en geleverd door externe aanbieders op basis van een individuele overeenkomst, bevat dit document strikte verplichtingen voor de aanbieder om de gebruiker (de notaris) in staat te stellen om de werking van het gebruikte systeem te verklaren. Als de notaris 'kant-en-klare' AI-oplossingen gebruikt moet de notaris uiterst voorzichtig te werk gaan en afzien van het gebruik van de specifieke AI als hij/zij zich zorgen maakt over het begrip vanwege het gebrek aan/beperkte transparantie en/of verklaarbaarheid.

Belangrijkste conclusies

- Transparantie en verklaarbaarheid van AI-systemen dragen bij aan de begrijpelijkheid ervan, het vergroten van het algemene vertrouwen in AI en aan de naleving van de regelgeving (zoals de AI Act).
- AI-transparantie en -verklaarbaarheid zijn verwant maar verschillend: verklaarbaarheid richt zich op het begrijpelijk maken van individuele outputs, transparantie zorgt voor duidelijkheid over de werking van het AI-systeem.
- Transparantie kan worden bereikt door nauwkeurige en uitgebreide documentatie en openbaarmaking van de belangrijkste aspecten van het betreffende AI-systeem.
- Een van de methoden voor AI-verklaarbaarheid is om complexe modellen uiteen te zetten om te identificeren hoe data en algoritme-eigenschappen bijdragen aan een specifieke output.
- De AI Act introduceert 3 niveaus van transparantieverplichtingen: algemene regels voor alle relevante AI-systemen, transparantieverplichting voor AI-systemen met een hoog risico, en aan de aanbieders van AI-modellen voor algemene doeleinden.
- Het black box-fenomeen is een obstakel voor AI-transparantie en -verklaarbaarheid. Dit betekent dat, door de ondoorzichtigheid van het AI-algoritme, niet alleen de gebruiker maar ook

de ontwikkelaars van het systeem kan niet volledig kunnen begrijpen waarom het tot een bepaalde conclusie kwam. De output van de black box AI is niet noodzakelijkerwijs incorrect, maar het fenomeen heeft een negatieve invloed op het benodigde vertrouwen in deze systemen.

- Notarissen moeten hun cliënten alleen informeren over de toegepaste technologische oplossingen als de relevante nationale bepalingen dit voorschrijven. Op basis van de AI Act moeten notarissen die bepaalde systemen met een hoog risico inzetten de betrokken personen hiervan op de hoogte stellen en hebben deze personen in bepaalde gevallen het recht om informatie te krijgen over de werking van het betreffende systeem.
- Notarissen moeten echter altijd de werking van het toegepaste AI-systeem en de redenen van zijn output begrijpen om vertrouwen te hebben in het gebruik van de specifieke AI-oplossing, om een betrouwbare en conforme eindbeslissing te nemen in het proces waarin de AI wordt gebruikt, en om het positieve imago van het beroep te behouden.
- Bij gebrek aan transparantie en/of verklaarbaarheid moeten notarissen de output van het gebruikte AI-systeem verwerpen en tijdig feedback geven aan de relevante aanbieder.

X. Human-in-the-loop—de rol van de notaris in een AI-gedreven wereld

1. Mogelijkheden en beperkingen van AI

Hoewel het in alledaags taalgebruik ‘artificiële intelligentie’ wordt genoemd, zijn AI-systemen niet intelligent in de menselijke betekenis van het woord. Volgens de definitie van het Oxford Advanced Learners’ Dictionary is intelligentie ‘*het vermogen om te leren, te begrijpen en op een logische manier over dingen na te denken*’. AI-systemen zijn in staat om gegevens te ‘leren’ en deze gegevens toe te passen op de manier waarop en voor de doeleinden waarvoor ze door menselijke ontwikkelaars zijn geprogrammeerd. AI heeft echter niet het vermogen om dingen te begrijpen en te denken zoals wij mensen dat doen. Daarom kan AI, ondanks de conventionele naamgeving, niet als intelligent worden beschouwd en blijft intelligentie voorlopig het exclusieve domein van de mens.

Huidige AI-systemen kunnen uitblinken in specifieke taken waarvoor ze getraind zijn. In principe zijn ze in staat om correcte en betrouwbare output te leveren met betrekking tot die taken. Dit vermogen van AI is echter sterk afhankelijk van investeringen: de systemen die meer financiële, menselijke en tijdsinvesteringen vergen (bijv. zelfrijdende auto’s, medische AI-oplossingen) en systemen waarbij grote belangen zijn gemoeid, zijn over het algemeen veel betrouwbaarder dan systemen die betrekking hebben op meer ‘marginale’ gebieden. Ondanks de hype rond ChatGPT en soortgelijke oplossingen van grote bedrijven bestaat er tegenwoordig geen algemene AI die in staat is om in alle domeinen de juiste output te leveren. AI-oplossingen die voor medische doeleinden zijn ontwikkeld, kunnen bijvoorbeeld niet worden gebruikt op juridisch gebied. Daarnaast, wat betreft het juridische vakgebied, is een AI-systeem getraind voor het helpen bij juridisch onderzoek waarschijnlijk niet de beste keuze om juristen te helpen bij het opstellen van rechtszaken die bij rechtbanken moeten worden aangespannen.

AI heeft andere belangrijke beperkingen waarmee rekening moet worden gehouden bij het gebruik van dergelijke systemen. Allereerst zijn de huidige AI-systemen niet in staat om situaties in een context te plaatsen zoals mensen dat doen. Bijvoorbeeld in het geval van rechtszaken kan

een AI-systeem de relevante bepalingen van de toepasselijke wetten en de bijbehorende jurisprudentie wel bieden, maar is deze niet in staat om de kenmerken van de gegeven situatie te begrijpen en rekening te houden met alle noodzakelijke factoren om een correcte en betrouwbare beslissing te maken of aan te bevelen.

Bovendien is AI niet in staat om enige creativiteit van het menselijke type te tonen, wat nodig is op juridisch gebied, vooral bij het bedenken van juridisch advies. AI kan ‘*hallucineren*’, wat verward kan worden met creatief zijn. Net als bij mensen is hallucinatie een negatief fenomeen, in tegenstelling tot de positief gekwalificeerde ‘*creativiteit*’. Achter menselijke creativiteit zit de beslissing van een mens om iets te creëren, en die beslissing dient daarbij niet voort te komen uit pure noodzaak. AI-hallucinatie, daarentegen, is het directe—zelfs negatieve—resultaat van de programmering van het algoritme.

Desondanks en ondanks de brede erkenning van de risico’s van AI-systemen is het fenomeen van automation bias, het overmatig vertrouwen op suggesties van digitale systemen, zeer sterk aanwezig en kan het zich ook voordoen op juridisch gebied. Zoals reeds vermeld in dit document, is het beste voorbeeld hiervan het geval van een advocaat in de Verenigde Staten die documenten indient bij de rechtbank, met jurisprudentie die is bedacht door ChatGPT. Dit enkele geval toont op zichzelf al aan dat de output van AI, hoe correct en overtuigend deze ook lijkt, niet blindelings kan worden vertrouwd. Een kritische benadering, grote zorgvuldigheid en strenge controle zijn nodig om situaties te vermijden die tot schadelijke gevolgen kunnen leiden. Dit benadrukt de centrale rol van de mens binnen het AI-ecosysteem, de zogeheten human-in-the-loop.

2. De rol van notarissen in een wereld met AI

Notarissen zijn zonder uitzondering volledig gekwalificeerde juridische professionals die hun beroep mogen uitoefenen na vele jaren juridische praktijkervaring en strenge examens. Al tientallen jaren vormen verschillende technologische oplossingen een belangrijk en noodzakelijk onderdeel van het notariële werk. Zonder hun inzet zou

den notariële procedures langzamer en minder efficiënt verlopen. Ondanks de redelijke aanvankelijke scepsis is het daarom ook voor het notariaat van cruciaal belang om technologische innovaties in te voeren en toe te passen, en AI kan hierop geen uitzondering vormen.

Benadrukt moet worden dat, op basis van de tekortkomingen van de AI-systemen die in dit handboek worden genoemd, AI momenteel niet in staat is notarissen (of vergelijkbare juridische beroepen) te vervangen of het beroep als geheel in gevaar te brengen. De samenleving staat over het algemeen sceptisch tegenover volledig geautomatiseerd genomen beslissingen.

De centrale aanwezigheid en activiteit van mensen is vereist (*“mensen willen advies van en beslissingen door mensen”*). Dit betekent uiteraard niet dat de maatschappij bezwaar heeft tegen de gepaste en voorzichtige inzet van geavanceerde technologische oplossingen in het menselijke besluitvormingsproces. AI-systemen bezitten echter niet de vaardigheden die een menselijke betrouwbare derde heeft (bijv. emotionele intelligentie, zich verplaatsen in de cliënt) en die, naast hun professionele kennis en ervaring, in hoge mate bijdragen aan het vertrouwen dat cliënten in notarissen stellen.

Daarom kan AI zelfs bij notariële activiteiten en procedures dienen als een hulpmiddel waarvan de mogelijkheden en beperkingen bekend moeten zijn bij notarissen, waarvan de inzet onder hun strikte menselijke toezicht moet staan en waarvan de output (beslissingen, aanbevelingen, etc.) grondig moet worden gecontroleerd en geverifieerd voordat deze wordt toegepast of weggegooid.

Dit betekent niet dat de rol van notarissen in een AI-gedreven wereld zal worden gereduceerd tot eenvoudige *‘controleurs’* van AI-outputs. AI kan het werk van notarissen versnellen door routinetaken (bijv. het verzamelen van basisinformatie over het onroerend goed waarop een notariële koopovereenkomst betrekking heeft) of administratieve taken (bijv. facturering of het regelen van een afspraak) uit te voeren waarvoor geen diepgaande juridische kennis nodig is. Bovendien kan het notarissen effectief helpen bij het vinden van relevante wettelijke bepalingen en jurisprudentie, wat de notaris veel tijd bespaart. De beoordeling van de gepaste aard van de output voor de betreffende context en de toepassing ervan hangt echter uitsluitend

af, en moet blijven afhangen, van de kennis, ervaring en deskundigheid van de notaris.

Op het gebied van notariële activiteiten kunnen de huidige AI-oplossingen geen taken vervullen die niet door de notaris zelf kunnen worden uitgevoerd. Het belangrijkste positieve verschil kan de snelheid zijn waarmee je tot een conclusie komt, net als bij een eenvoudige rekenmachine: mensen zijn in staat om zeer complexe wiskundige oefeningen uit te rekenen, de rekenmachine versnelt alleen het proces van tellen. Maar in tegenstelling tot bij rekenen is er notariële zaken bijna nooit slechts één oplossing voor een zaak, maar meerdere. Daarom heeft de output van de toegepaste AI een andere weging dan de output van een rekenmachine. Dit betekent dat, net als bij elke andere technische oplossing, AI het werk van de notaris aanvult. Net als bij producten met geïntegreerde AI moeten notarissen in staat zijn om *‘op de stopknop te drukken’* en de output van de AI-systemen afwijzen.

3. Werken met AI

Zowel bij intern (door notariële organisaties) ontwikkelde of extern ingekochte AI-oplossingen is het belangrijk dat notarissen vanaf het begin betrokken zijn. Notarissen kunnen hun behoeften en het doel waarvoor ze een AI-systeem willen gebruiken identificeren en vervolgens actief deelnemen aan het testproces van de betreffende oplossing (bijv. in sandboxes).

Notariële organisaties hebben de taak om de AI-geletterdheid van notarissen te vergroten door hen te trainen in hoe en in welke situaties AI-systemen kunnen worden gebruikt. In het geval van generatieve AI-modellen, waarbij de kwaliteit (bijv. relevantie, volledigheid) van de prompts van de gebruiker cruciaal is om de juiste output te krijgen, moeten notarissen getraind worden in het juist formuleren van hun prompts.

Tot slot is feedback van notarissen cruciaal om in de praktijk de onverwachte beperkingen en tekortkomingen van het gebruikte AI-systeem te ontdekken. Daarom moeten notarissen een gebruiksvriendelijke manier krijgen om dergelijke informatie snel te melden aan de notariële organisaties waarvan ze lid zijn en aan de bevoegde dienstverleners.

Notarissen moeten ernaar streven alleen gebruik te maken van de best mogelijke AI-oplossingen die transparant en verklaarbaar zijn en moeten afzien van het gebruik van systemen waarvan de betrouwbaarheid niet kan worden gecontroleerd en waarbij het er ook maar enig risico bestaat dat een belangrijke notariële verplichting wordt geschonden (bijv. schending van het beroepsgeheim).

Belangrijkste conclusies

- AI is geen intelligentie in de menselijke betekenis van het woord. AI is niet in staat om te begrijpen en te denken.
- Huidige AI-systemen zijn niet in staat om dingen in een context te plaatsen en creatief te zijn.
- AI-systemen kunnen uitblinken in taken waarvoor ze getraind zijn, maar op dit moment bestaat er geen algemene AI die in staat is om nauwkeurige en betrouwbare resultaten te leveren op elk gebied van het leven.
- Automation bias, ofwel overmatig vertrouwen op de suggesties van technologische oplossingen, moet worden vermeden. De betrouwbaarheid van AI-output moet altijd worden geverifieerd. Desondanks is het omarmen en toepassen van technologische innovaties (waaronder AI) ook voor het notariële beroep cruciaal.
- Op dit moment is er geen AI-oplossing die kan dienen als vervanging voor een notaris.
- Klanten hebben menselijke interacties en beslissingen nodig evenals de aanwezigheid en toepassing van vaardigheden (zoals empathie) die alleen mensen bezitten.
- Huidige AI-oplossingen kunnen geen taken vervullen die niet door de notaris zelf kunnen worden uitgevoerd.
- AI kan dienen als hulpmiddel voor notarissen. De inzet van AI-systemen moet onder streng menselijk toezicht staan en de output moet grondig worden gecontroleerd en geverifieerd voordat deze wordt toegepast of weggegooid.
- Notarissen moeten een actieve rol spelen bij het bepalen van het doel van de AI-oplossingen die ze gaan gebruiken en bij het testen van dergelijke systemen. Notarissen moeten regelmatig feedback geven over dergelijke AI-systemen.
- De AI-geletterdheid van de notarissen moet worden verbeterd voor een efficiënt en veilig gebruik van AI-systemen.

XI. Intellectueel eigendom en artificiële intelligentie

1. Algemene inzichten – Identificatie van de relevante IP-rechten in notarieel-AI-verband

Er zijn verschillende soorten intellectueel eigendom (IP), waarvan de meest voorkomende het auteursrecht en naburige rechten, het ‘*sui generis*’ databankrecht, het handelsmerk en het octrooi zijn. AI deze soorten IP hebben verschillende beschermingsonderwerpen en komen in verschillende situaties voor. AI heeft specifieke verbanden en problemen met elk van deze IP-rechten die specifiek bekeken moeten worden.

In de context van het notariaat en AI hebben het auteursrecht en het ‘*sui generis*’ databankenrecht het grootste belang, aangezien auteursrechtelijk beschermde werken en databanken dagelijks worden gebruikt en kunnen worden geproduceerd in de notariële praktijk. Daarom richt dit hoofdstuk zich uitsluitend op deze twee intellectuele eigendomsrechten.

2. Auteursrecht op notariële akten, rechtsinstrumenten en databanken voor AI

a) Auteursrecht en notariële akten

Auteursrecht is een breed geharmoniseerd gebied binnen de Europese Unie. Ondanks het naast elkaar bestaan van de nationale auteursrechtssystemen, vormen de beschermings-criteria en de belangrijkste termen met betrekking tot het gebied autonome Europese concepten die uniform moeten worden toegepast in de 27 lidstaten. Het auteursrecht wordt echter gekenmerkt door het territorialiteitsbeginsel, wat betekent dat naast de EU-wetgeving de nationale regels grondig moeten worden nageleefd vanwege bepaalde verschillen die niet geharmoniseerd zijn op EU-niveau. Daarom wordt in dit hoofdstuk de relevante EU-wetgeving gepresenteerd en worden enkele punten genoemd die kunnen worden gebruikt om de juridische situatie in de verschillende lidstaten te controleren.

Het belangrijkste criterium voor auteursrechtelijke bescherming in de hele EU is de originaliteit van het werk. Om de voordelen van het auteursrecht te genieten, moet het specifieke werk ‘*origineel*’ zijn. Deze eenvoudige term is uitgelegd in de Infopaq I-beschikking van het Europese Hof van Justitie. In de Infopaq I-beschikking werd “*originaliteit*” omschreven als “*de eigen intellectuele schepping van de auteur*”. Dit is een relatief lage beschermingsdrempel en aangezien de geldelijke waarde, de esthetische kenmerken van het werk en de hoeveelheid tijd, moeite en energie die in de creatie is gestoken geen rol kunnen spelen bij de kwalificatie van auteursrechtelijke bescherming, vallen veel werken onder het auteursrecht. Bovendien is het een basisprincipe dat pure ideeën geen auteursrechtelijke bescherming kunnen genieten; ze moeten in een of andere vorm worden uitgedrukt (bijvoorbeeld op schrift) om dit te bereiken.

Het originaliteitscriterium leidt er in principe toe dat authentieke notariële akten auteursrechtelijk beschermd kunnen zijn zodra het gaat om “*eigen intellectuele schepping van de auteur [in dit geval de notaris]*”. Daarentegen kunnen bepaalde sjablonen en formulieren die in de notariële praktijk worden gebruikt (bijv. de Europese erfrechtverklaring) niet auteursrechtelijk worden beschermd, omdat ze niet voldoen aan het criterium van originaliteit (en vaak maken ze deel uit van officiële rechtshandelingen die gewoonlijk buiten het toepassingsgebied van het auteursrecht vallen).

Ondanks de harmonisatie op EU-niveau blijft auteursrecht echter een nationaal gebied en moet de relevante wetgeving van het land van de notaris worden gecontroleerd om na te gaan of notariële handelingen al dan niet zijn uitgesloten van auteursrechtelijke bescherming (in sommige landen zijn officiële documenten van overheidsinstanties bijvoorbeeld uitgesloten van auteursrecht). Afhankelijk van de nationale wetgeving die van toepassing is op de notariële akten, is het ook mogelijk dat—als de bescherming van toepassing is—de economische rechten van het auteursrecht op deze akten (bijvoorbeeld het recht op reproductie) worden overgedragen aan de respectieve cliënten van de notaris tegen betaling van de notariskosten.

Als in een nationaal rechtssysteem de auteursrechtelijke bescherming van notariële akten niet is uitgesloten, kan dit gevolgen hebben voor het gebruik daarvan in de context van AI. In principe is hun reproductie voor het trainen van (notariële) AI-systemen onderworpen aan autorisatie (licentie). Bovendien, zoals aangegeven in de relevante hoofdstukken van dit Handboek, kunnen persoonsgegevens en handelsgeheimen ook een belemmering vormen voor het gebruik van notariële akten als trainingsmateriaal voor AI, en zou moeten worden nagegaan of zelfs de notariële organisaties waarvan de notaris lid is, toegang mogen hebben tot de inhoud en/of metagegevens van de op papier of elektronisch gearchiveerde akten.

b) Bescherming van juridische teksten en jurisprudentie

Daarnaast worden aan de ‘input’-kant van de notariële praktijk voortdurend juridische teksten en jurisprudentie gebruikt. Om praktische redenen en vanwege hun publieke belang voor de samenleving vallen officiële juridische teksten en jurisprudentie in de meeste landen buiten de bescherming van het auteursrecht. Deze rechtsbronnen moeten vrij toegankelijk zijn en hun reproductie moet zonder beperkingen worden toegestaan, zodat burgers en rechtspersonen hun rechten kunnen uitoefenen en hun plichten kunnen nakomen. Dit betekent dat deze teksten vrijelijk kunnen worden gebruikt (bijv. gereproduceerd), ook voor AI-training, in ons geval voor de training van notariële AI-systemen. Maar ook in dit geval moet de relevante nationale wetgeving inzake auteursrecht altijd grondig worden onderzocht.

c) Bescherming van databanken

Juridische en niet-juridische databanken—regelmatig gebruikt door notarissen—kunnen op twee verschillende manieren beschermd worden: het ‘algemene’ auteursrecht beschermt de databank als deze origineel is in zijn selectie, coördinatie en ordening. Dit beschermt de structuur van de databank, niet de inhoud (wat werken zonder auteursrechtelijke bescherming kunnen zijn). Dit resulteert er onder andere in dat alleen al de alfabetische rangschikking van gegevens niet origineel genoeg is voor bescherming van de databank door het ‘algemene’ auteursrecht.

Voor databanken die het vereiste niveau van originaliteit niet halen, introduceerde de Europese wetgever echter het zogenaamde *sui generis* databankrecht. Deze ‘*sui generis*’ bescherming wordt verleend om de substantiële investering (financieel, materieel en/of menselijk) in het verkrijgen, verifiëren of presenteren van de inhoud van de databank te respecteren. In tegenstelling tot het ‘algemene’ auteursrecht beschermt het ‘*sui generis*’ recht de inhoud van de databank en geeft het een bescherming van 15 jaar die begint op de datum van creatie of van de eerste beschikbaarstelling aan het publiek. Beide soorten bescherming kunnen er in principe toe leiden dat het reproduceren van dezelfde databank, het extraheren of hergebruiken van de volledige inhoud of van een substantieel deel van de inhoud van de databank voor (notariële) AI-training een schending is van het auteursrecht of het ‘*sui generis*’ databankrecht.

3. Uitzondering en beperking van tekst- en datamining voor AI-training

Gebaseerd op de algemene regels van het auteursrecht (Artikel 2 van Richtlijn 2001/29/EG van het Europees Parlement en de Raad van 22 mei 2001 betreffende de harmonisatie van bepaalde aspecten van het auteursrecht en naburige rechten in de informatiemaatschappij, kortweg: de InfoSoc-Richtlijn), heeft de auteur van het respectieve werk het exclusieve reproductierecht met betrekking tot het geheel of een deel van zijn/haar werk. Reproductie van het werk kan worden toegestaan aan derden, voornamelijk door middel van licenties. Zoals vermeld onder het vorige punt, heeft de fabrikant van de databank in het geval van het ‘*sui generis*’ databankrecht het exclusieve recht om de extractie en/of het hergebruik van de volledige inhoud van de databank of een substantieel deel daarvan te voorkomen.

Rekening houdend met de extreem grote hoeveelheid gegevens (waaronder auteursrechtelijk beschermde werken) die nodig is voor AI-training zou het telkens en voor elk werk eisen en verstrekken van een licentie buitensporig belastend zijn voor de AI-ontwikkelaars en aanbieders, evenals voor de rechthebbenden. Aangezien het gebruik van werken echter kan worden beschouwd als ongeoorloofde reproductie en ongeoorloofd hergebruik, zouden de exclusieve rechten van de rechthebbenden—zonder specifieke wetgevende tussenkomst—juridische obstakels vormen voor het trainen van AI-modellen. Dit zou niet alleen de ontwikkeling van AI-modellen belemmeren, maar kan

ook het AI-innovatie- en ecosysteem als geheel in gevaar brengen.

Om hier een oplossing voor te vinden, heeft de EU-wetgever in 2019 de zogenaamde uitzonderingen en beperkingen voor tekst- en datamining (TDM) ingevoerd in de Richtlijn inzake auteursrechten in de digitale eengemaakte markt. Overeenkomstig artikel 4 voorzien de lidstaten in een beperking of restrictie van onder meer de exclusieve rechten op reproductie en extractie van auteursrechtelijk beschermde werken en gegevens uit de databanken die door het recht *sui generis* worden beschermd, ten behoeve van TDM. Het doel van deze bepaling is om de AI-ontwikkelaars en aanbieders te bevrijden van de bovengenoemde licentieverzoeken.

Deze TDM-regel kent geen beperking met betrekking tot de entiteit die er gebruik van maakt, wat ertoe leidt dat AI-modellen ontwikkeld door het notariaat onder het toepassingsgebied kunnen vallen en de beroepsgroep er gebruik van kan maken. Daarnaast zijn het doel en de aard (commercieel of niet-commercieel) van de TDM niet beperkt en stelt de bepaling alleen de rechtmatige toegang tot het gegeven werk/de gegeven database als vereiste. Echter de reikwijdte van deze uitzondering of beperking wordt beperkt door de opt-out-mogelijkheid die kan worden uitgeoefend door de betreffende rechthebbende (auteur van het werk, maker van de databank, inclusief de notaris wiens handelingen onder auteursrechtelijke bescherming kunnen vallen op grond van het toepasselijke recht), waardoor het opnieuw noodzakelijk wordt om toestemming te vragen voor gebruik voor TDM-doeleinden.

In het geval van inhoud die online openbaar beschikbaar is gemaakt, kunnen de bovenstaande rechten worden voorbehouden door het gebruik van machineleesbare middelen, waaronder metagegevens en voorwaarden van een website of dienst. In andere gevallen kan het voorbehoud worden gemaakt door bijvoorbeeld contractuele overeenkomsten of een eenzijdige verklaring. In het geval van notariële AI-ontwikkeling—naast de rechtmatige toegang tot het materiaal—moet de opt-out die door de rechthebbende wordt uitgeoefend, worden gecontroleerd en gerespecteerd. Als de opt-out wordt uitgesproken, moet het materiaal voor TDM en AI-training worden weggegooid, of het notariaat dat het systeem ontwikkelt moet een licentie krijgen voor dergelijk gebruik. Als er geen opt-out wordt uit-

geoefend, is de ontwikkelaar vrij om het betreffende werk te gebruiken voor AI-training.

Bovendien bevat artikel 53 van de AI Act ‘spiegel’-auteursrechtbepalingen voor het geval de (notariële) AI-training een AI-model voor algemene doeleinden is. In dit geval is de aanbieder verplicht om een beleid in te voeren om te voldoen aan de wetgeving van de Unie inzake auteursrecht en in het bijzonder om het opt-out-recht van de Richtlijn inzake auteursrechten in de digitale eengemaakte markt na te leven en om een voldoende gedetailleerd overzicht op te stellen en openbaar te maken van de inhoud die wordt gebruikt voor training van het AI-model voor algemene doeleinden, met gebruikmaking van sjablonen verstrekt door de AI Office. Het doel van deze bepaling is om houders van rechten in staat te stellen om het gebruik van hun werken voor AI-training te identificeren.

4. Auteursrechtelijke bescherming van AI-output

Binnen de EU is auteursrechtelijke bescherming uitsluitend van toepassing op door mensen gemaakte werken, wat betekent dat werken die door AI zijn gegenereerd buiten het auteursrecht vallen. Werken die met behulp van AI zijn gemaakt, kunnen echter wel auteursrechtelijk worden beschermd als ze voldoen aan de originaliteitscriteria, d.w.z. als het gaat om ‘*eigen intellectuele scheppingen van de auteur*’.

Zoals vermeld in verschillende hoofdstukken van dit Handboek, is de notariële (menselijke) controle en correctie van de output van AI-oplossingen onmisbaar, en rekening houdend met de rol en mogelijkheden van de AI (hulpmiddel om het werk te vergemakkelijken en te stroomlijnen, gebrek aan begrip van de context, etc.) is het vrij onrealistisch dat notarissen de output van de AI één-op-één overnemen zonder correcties, aanvullingen, wijzigingen. Hoe complexer het beoogde resultaat, hoe groter de kans op significante menselijke interventie. Daarom dient de AI in deze gevallen slechts als hulpmiddel, met inachtneming van de bepalingen van de nationale auteursrechtwetgeving. Documenten geproduceerd door de notaris met AI-ondersteuning (authentieke akte, juridisch advies, onderzoek, etc.) kunnen onder auteursrechtelijke bescherming vallen.

Tegelijkertijd, als de AI-output precies hetzelfde is als of in wezen lijkt op een eerder gecreëerd werk en de onafhankelijke, dubbele creatie (productie van hetzelfde of in wezen gelijksoortig werk zonder enig verband tussen de twee werken en auteurs) niet kan worden bewezen, kan er een risico op inbreuk op het auteursrecht bestaan. Daarom wordt (gedeeltelijke) herformulering van de gegeven AI-output door de notaris volgens zijn/haar professionele methoden, eigen stijl en woordenschat sterk aanbevolen.

Belangrijkste conclusies

- In de context van AI in het notariaat zijn de meest relevante intellectuele eigendomsrechten het auteursrecht en het ‘*sui generis*’ databankrecht.
- Auteursrecht is een gedeeltelijk geharmoniseerd gebied, maar het territorialiteitsbeginsel geldt, waardoor naast de EU-wetgeving ook de nationale regels van de respectieve landen moeten worden gecontroleerd.
- Het belangrijkste criterium voor auteursrechtelijke bescherming is dat het werk origineel moet zijn, d.w.z. ‘*de eigen intellectuele schepping van de auteur*’. De auteur heeft het exclusieve recht om het werk geheel of gedeeltelijk te reproduceren.
- Afhankelijk van de nationale wetgeving kunnen notariële akten die voldoen aan het originaliteitscriterium auteursrechtelijke bescherming genieten, wat het gebruik ervan voor (notariële) AI-training kan belemmeren.
- In het algemeen—maar ook afhankelijk van de nationale wetgeving—vallen officiële rechtshandelingen en jurisprudentie buiten het auteursrecht, wat betekent dat deze teksten zonder toestemming kunnen worden gebruikt voor AI-training, ook binnen het notariaat.
- De IP-bescherming van databases is tweeledig in de EU. De ‘*algemene*’ auteursrechtelijke

bepalingen zijn van toepassing (criterium van originaliteit) op de selectie, coördinatie en ordening van de gegevens. Anderzijds wordt het ‘*sui generis*’ databankrecht verleend om de substantiële investering (financieel, materieel en/of menselijk) in het verkrijgen, verifiëren of presenteren van de inhoud van de databank te respecteren. Beide beschermingsrechten kunnen leiden tot inbreuk in geval van (notariële) AI-training.

- Er is een extreem grote hoeveelheid gegevens (waaronder auteursrechtelijk beschermde werken) nodig voor AI-training, waardoor het voor elk werk eisen en verstrekken van een licentie buitensporig belastend zou zijn voor de AI-ontwikkelaars en aanbieders, evenals voor de rechthebbenden.
- Om te voorkomen dat rechten worden geschonden en om de AI-ontwikkelingen te vergemakkelijken, moesten de lidstaten een tekst- en datamining uitzondering of beperking introduceren met een opt-out-mogelijkheid voor de rechthebbende.
- Door AI gegenereerde werken zijn niet auteursrechtelijk beschermd in de EU, maar door AI geassisteerde werken mogelijk wel.
- Het wordt notarissen aanbevolen om de door AI geassisteerde output (gedeeltelijk) te herformuleren om elk risico op schending van het auteursrecht te vermijden.

XII. Kant-en-klare, intern ontwikkelde en extern geleverde AI-systemen

1. ‘Kant-en-klare’ AI-systemen

De juridische sector, met name het notariaat, heeft tal van specifieke kenmerken die van invloed zijn op de keuze van de toe te passen technologische hulpmiddelen. ‘Kant-en-klare’ softwaretools, websites en andere toepassingen (waaronder AI-systemen, zoals ChatGPT, DeepL of Microsoft Copilot) die gratis of tegen betaling online aan het publiek worden aangeboden, kunnen door notarissen worden gebruikt voor bepaalde specifieke taken. Ze zijn over het algemeen zeer kosteneffectief in vergelijking met op maat gemaakte systemen. Bovendien wordt de ontwikkeltijd van dergelijke oplossingen gespaard omdat ze meestal onmiddellijk toegankelijk en toepasbaar zijn. Ook de mogelijke mislukkingen van de ontwikkeling en de behoefte aan algoritmecorrecties zijn voor rekening van de aanbieder.

De risico's van het standaard gebruiken van dergelijke AI-oplossingen binnen het notariaat zijn echter extreem hoog en overtreffen meestal de potentiële voordelen. De aanbieders van deze oplossingen passen hun algemene voorwaarden toe die eenzijdig door hen zijn opgesteld en waarin hun klanten geen speelruimte hebben. Bovendien is er meestal geen garantie dat de ‘kant-en-klare’ tools de bescherming van persoonsgegevens of handelsgeheimen garanderen, wat cruciaal is voor beroepen zoals het notariaat. Daarnaast kunnen door notarissen gegenereerde gegevens (bijv. door hen geformuleerde contractbepalingen) die niet in de voorgaande categorieën vallen en als invoer worden gebruikt (bijv. in automatische vertaaloplossingen) ook het risico lopen verder te worden gebruikt voor het trainen van dergelijke systemen. Bovendien kunnen de bronnen, de wettigheid en de kwaliteit van de gegevens die door dergelijke systemen worden gebruikt vaak niet worden geverifieerd, wat kan leiden tot problemen in verband met inbreuk op het auteursrecht, en tot bias. Ook al zijn verschillende van deze oplossingen open source, toch hebben aanbieders hun eigen handelsgeheimen die het, bovenop het *‘black box’-probleem*, uiterst moeilijk maken om de werking van het onderliggende algoritme te begrijpen en om uit te leggen waarom het systeem tot een bepaalde conclusie kwam (probleem van transparantie en verklaarbaarheid).

Het wordt notarissen niet volledig afgeraden om ‘kant-en-klare’ AI-systemen te gebruiken, maar ze worden wel sterk aangeraden om deze met de grootst mogelijke voorzichtigheid in te zetten. In verschillende hoofdstukken van dit Handboek worden de risico's (bijv. bescherming van persoonsgegevens behandeld waarmee rekening moet worden gehouden bij het gebruik van AI-oplossingen. Deze risico's kunnen exponentieel toenemen wanneer ‘kant-en-klare’ AI wordt gebruikt. Als het risico niet kan worden vermeden of tot een minimum kan worden beperkt, wordt aangeraden het specifieke systeem niet te gebruiken.

2. Voordelen en moeilijkheden van intern ontwikkelde AI-oplossingen voor notarissen

Er zijn specifieke notariële gebieden en zaken waarbij ‘kant-en-klare’ AI-systemen geen adequate en efficiënte hulp kunnen bieden. Dit zijn meestal generieke systemen die niet zijn afgestemd op de juridische sector en al helemaal niet op het notariaat (ChatGPT is bijvoorbeeld zeer beperkt in het correct opstellen van notariële akten). Daarom kunnen in bepaalde gevallen alleen op maat gemaakte, intern ontwikkelde notariële AI-systemen de noodzakelijke oplossing bieden. Interne AI-ontwikkeling in deze context betekent de ontwikkeling van AI-systemen uitsluitend door de betreffende notariële organisatie. Dit punt heeft uitsluitend betrekking op notariële organisaties, aangezien het niet realistisch is—vooral vanwege de kosten die dit met zich meebrengt (zie hieronder)—dat individuele notarissen hun eigen AI-oplossingen ontwikkelen. Notariële AI-systemen die intern door en voor de beroepsgroep worden ontwikkeld, hebben het inherente voordeel dat ze de in punt 1 van dit hoofdstuk genoemde problemen op efficiënte wijze vermijden of beperken.

Notarissen verzamelen elke dag een enorme hoeveelheid gegevens. Deze gegevens zijn beroepsspecifiek en daarom altijd relevant en nauwkeurig. Notariële AI-oplossingen moeten vooral worden getraind op gegevens die afkomstig zijn van de beroepsgroep en van bronnen die kwaliteitsgegevens leveren en waartoe de beroepsgroep

wettelijk toegang heeft. Dit garandeert dat de intellectuele eigendomsrechten en verschillende rechten op gegevens niet worden geschonden, dat de kwaliteit van de gegevens goed is en dat de output van het systeem op basis van gegevens niet onjuist is. Bovendien kan de bescherming van de persoonsgegevens, handelsgeheimen en het beroepsgeheim van notarissen efficiënt worden gewaarborgd door technische oplossingen in het specifieke AI-systeem.

Het probleem dat zich in dit geval kan voordoen, is de toegang tot de gegevens van individuele notarissen door de bevoegde notariële organisatie die het AI-systeem ontwikkelt. Daarom is het mogelijk dat notariële organisaties geen of beperkte toegang hebben tot dergelijke gegevens of er alleen toegang toe hebben na ze eerst voldoende te hebben bewerkt (bijvoorbeeld afgeschermd). Daarom moet altijd rekening worden gehouden met de relevante nationale beperkingen. Als er in dit opzicht beperkingen zijn, kan het gebruik van sjablonen, uittreksels en soortgelijke anonieme documentatie opgesteld door de beroepsgroep of synthetische gegevens een oplossing bieden voor het trainen van het betreffende systeem. In landen waar notariële organisaties toegang hebben tot de relevante gegevens—om de intellectuele autonomie (bijv. individueel geformuleerde contractuele clausules) van notarissen te respecteren—moeten zij bovendien de mogelijkheid krijgen om van de respectieve organisatie te eisen dat hun akten, bepaalde akten of delen daarvan worden weggelaten bij het trainen van AI-systemen. Deze mogelijkheid moet ook worden geboden in gevallen waarin het betreffende land de notariële akten niet kwalificeert als auteursrechtelijk beschermde werken waarvoor TDM opt-out kan worden uitgeoefend.

Zoals vermeld in het relevante hoofdstuk kan AI bias niet volledig worden verwijderd uit de systemen—vanwege het feit dat het een inherent biologisch kenmerk van mensen is—maar het beperken van bias en mogelijke hallucinatie kan efficiënter en sneller worden uitgevoerd in het geval van intern ontwikkelde notariële systemen. Door ingebouwde feedbackmechanismen te introduceren, kunnen notarissen directe en indirecte feedback geven en de ontwikkelaar informeren over hun praktijkervaring met de gegeven oplossing, waardoor het AI-systeem efficiënter en nauwkeuriger wordt.

Aangezien de controle van de ontwikkeling en actualisering van deze systemen in handen is van de beroepsgroep, kan de transparantie en verklaarbaarheid van der-

gelijke systemen vanaf de eerste stap van de ontwikkeling worden gegarandeerd, waardoor het *'black box-probleem'* wordt vermeden.

De intern ontwikkelde AI-oplossingen kunnen ook worden geïntegreerd in de reeds gebruikte digitale notariële administratietools, waardoor de interoperabiliteit van dergelijke systemen met de reeds toegepaste digitale oplossingen wordt gewaarborgd. De notariële organisatie die een AI-oplossing aanbiedt, moet zorgen voor de benodigde training voor notarissen en de werknemers van notarissen die dergelijke systemen gebruiken en beschikbaar blijven om zo nodig technische problemen op te lossen.

Tegelijkertijd moet er rekening mee worden gehouden dat de ontwikkeling van AI-systemen kostbaar is, vooral als het gaat om geavanceerde oplossingen zoals LLM's en generatieve AI-systemen. Het van de grond af ontwikkelen van AI-oplossingen vergt over het algemeen veel tijd (ontwikkeling, training, validatie, testen etc.). Bovendien vereisen dergelijke ontwikkelingen IT-specialisten en -expertise. Als een ontwikkeld AI-systeem onder de categorie hoog risico van de AI Act valt, dan moet de notariële organisatie als aanbieder voldoen aan een groot aantal eisen (zie het desbetreffende hoofdstuk). Momenteel beschikken niet alle notariële organisaties over de nodige financiële/technologische/menselijke middelen om dergelijke systemen op te zetten, wat ertoe kan leiden dat ze een beroep moeten doen op externe dienstverleners.

3. Notariële AI-systemen geleverd door externe dienstverleners (AI as a Service)

Indien een notariële organisatie of de individuele notaris (de twee onder dit punt verder aangeduid als: 'gebruiker') zich tot een externe dienstverlener wendt voor het ontwikkelen en aanbieden van een specifiek AI-systeem zijn de twee belangrijkste stappen de zorgvuldige keuze van de dienstverlener en de onderhandeling over individuele contractvoorwaarden (AI as a Service - *AaaS*-contracten).

Heel vaak—vooral als de dienstverlener geen bekend bedrijf is—is het uitvoeren van due diligence op de dienstverlener uiterst nuttig om de risico's te beoordelen die het beroep op de dienstverlener met zich meebrengt. In het geval dat de resultaten van de due diligence niet voldoende de betrouwbaarheid en deskundigheid van de aanbieder

aantonen, is het sterk aan te raden om verder te zoeken naar een andere aanbieder om volledig te voldoen aan de behoeften van de gebruiker.

In het AlaaS-contract moet de gebruiker duidelijk bepalen en in detail communiceren wat het precieze doel is van het systeem dat ontwikkeld moet worden door de aanbieder en wat de kenmerken zijn, alsmede de regelgeving rondom de activiteit waarin het AI-systeem de gebruiker gaat assisteren.

Naast de gebruikelijke voorwaarden in contracten moeten clausules over de volgende zaken worden opgenomen in het AlaaS-contract (de lijst is niet uitputtend: afhankelijk van de omstandigheden, de behoeften van de gebruiker, de nationale regelgeving en andere zaken kunnen andere of afwijkende clausules nodig zijn):

- Vereisten voor gegevenskwaliteit om ervoor te zorgen dat de gegevens die worden gebruikt voor de training en werking van het systeem geschikt zijn voor het doel;
- Criteria voor de bronnen van trainingsdata om te garanderen dat de gegevens afkomstig zijn van legale en wettelijk erkende bronnen;
- Rechten (inclusief IP-rechten) op de trainingsdata, invoer- en uitvoergegevens om ervoor te zorgen dat de aanbieder geen rechten krijgt op de gegevens die door de gebruiker worden aangeleverd en op de gegevens in prompts en op de outputgegevens van het systeem. Bovendien is het sterk aan te raden om in het contract te vermelden dat geen van de gegevens door de aanbieder kan worden gebruikt voor het trainen van andere AI-systemen;
- Intellectuele eigendomsrechten (inclusief auteursrecht, patent, handelsmerken) met betrekking tot het systeem en de onderdelen van het geleverde systeem;
- Bescherming van persoonsgegevens om te garanderen dat de relevante regels van de AVG naar behoren worden nageleefd wanneer persoonsgegevens van cliënten van notarissen worden ingevoerd in het AI-systeem;
- Bescherming van de beroepsgeheimen, handelsgeheimen en andere vertrouwelijke gegevens om ervoor te zorgen dat de geheimhouding van dergelijke gegevens van cliënten en van de gebruikers wordt bewaard;

- Verplichting tot transparantie van het AI-systeem en de verklaarbaarheid van de output om ervoor te zorgen dat de werking van het systeem en de productie van de output duidelijk en begrijpelijk is voor de gebruikers;
- Verplichting om het systeem regelmatig bij te werken en te onderhouden, waaronder het bijwerken van de trainingsdataset en het technologisch bijwerken van het gebruikte algoritme met aanvullende informatieplicht vóór de geplande bijwerking en na de voltooiing ervan;
- Zorgen voor compatibiliteit en interoperabiliteit met andere digitale systemen die de betreffende gebruiker gebruikt om de AI-oplossing soepel in dergelijke systemen te kunnen integreren;
- Tijdig ingrijpen bij defecten en storingen van het systeem, waaronder de-biasing en het beperken van AI-hallucinaties;
- Verplichting om de gebruikers te trainen in het juiste gebruik en de specifieke kenmerken van het systeem;
- Maatregelen nemen om het juiste niveau van cyberveiligheid te bereiken;
- Bepaling van aansprakelijkheid en volledige schade-loosstelling in geval van schade als gevolg van de tekortkomingen en/of het slecht functioneren van het systeem;
- Voorzieningen met betrekking tot aanbiedingen van derden (d.w.z. wanneer het systeem van de aanbieder zal worden gebruikt in combinatie met een systeem van een andere aanbieder als een dienst die erop is gebouwd), om te voorkomen dat er onderliggende problemen ontstaan die verband houden met de vorige punten vanwege de voorwaarden met derden;
- Naleving van andere bepalingen die worden vereist door de relevante wetgeving (bijv. het voldoen aan de registratieverplichting onder de AI Act voor AI-systemen met een hoog risico in de EU-databank door aanbieders van dergelijke systemen).

Tot slot, rekening houdend met de definities van ‘aanbieder’ en ‘gebruiker’ in de AI Act moet worden bepaald of een notariële organisatie die een externe aanbieder vraagt om een AI-systeem te ontwikkelen voor de notarissen die lid zijn van deze organisatie dat buiten het materiële toepassingsgebied van de AI Act valt wordt beschouwd als een aanbieder of gebruiker. Dit is een belangrijk verschil met de

uitgebreidere nalevingsverplichtingen van de aanbieders dan van de gebruikers met betrekking tot AI-systemen met een hoog risico.

In overeenstemming met artikel 3, lid 3, van de AI Act, valt onder ‘aanbieder’ ook een entiteit die een AI-systeem laat ontwikkelen dat zij onder haar eigen naam of handelsmerk, al dan niet tegen betaling, in gebruik neemt. Onder ingebruikneming wordt volgens lid 11 van hetzelfde artikel verstaan: de levering van een AI-systeem voor eerste gebruik rechtstreeks aan de gebruiker of voor eigen gebruik in de Unie voor het beoogde doel. In deze situatie moeten de gebruikers van het AI-systeem zeker de notarissen zijn, en de ingebruikname zou ook kunnen plaatsvinden, omdat

de notariële organisatie het AI-systeem voor het eerste gebruik rechtstreeks aan de gebruikers (notarissen) levert. Als de betreffende notariële organisatie het systeem echter niet onder haar eigen naam of handelsmerk in gebruik zou nemen (het is waarschijnlijk dat de naam of het handelsmerk van de ‘echte’ en oorspronkelijke aanbieder in het product wordt vermeld), is de kwalificatie als aanbieder niet van toepassing. Daarom moet in deze situatie de relevante bepaling van het AlaaS-contract (over de vermelding van de naam en/of het handelsmerk van de ontwikkelaar/originele aanbieder) zorgvuldig worden geformuleerd, waarbij de naam en/of het handelsmerk van de externe aanbieder wordt vermeld.

Belangrijkste conclusies

- ‘Kant-en-klare’ softwaretools, websites en andere toepassingen die gratis of tegen betaling online aan het publiek worden aangeboden, kunnen door bedrijven worden gebruikt voor bepaalde specifieke taken.
- De risico's van dergelijke systemen (bijv. bescherming van persoonsgegevens, slechte kwaliteit van gegevens) overtreffen meestal hun potentiële voordelen voor het notariaat.
- Het wordt notarissen niet volledig afgeraden om ‘kant-en-klare’ AI-systemen te gebruiken, maar het wordt wel sterk aangeraden om deze met de grootst mogelijke voorzichtigheid in te zetten. Als het risico niet kan worden vermeden of tot een minimum kan worden beperkt, wordt de notaris aangeraden het specifieke systeem niet te gebruiken.
- In bepaalde gevallen kunnen alleen op maat gemaakte, internontwikkelde notariële AI-systemen notarissen de juiste hulp bieden.
- Intern ontwikkelde notariële AI-systemen kunnen de kwaliteit van de gebruikte gegevens, de bescherming van persoonsgegevens, van handelsgeheimen en beroepsgeheimen van cliënten, de snelle reactie op bias en hallucinatie, transparantie en verklaarbaarheid, en de compatibiliteit en interoperabiliteit met andere digitale notariële systemen garanderen.
- Intern ontwikkelde notariële AI-systemen hebben ook bepaalde nadelen, waaronder de hoge kosten, de lange tijd en het IT-personeel die nodig zijn voor de ontwikkeling.
- Als een notariële organisatie of een individuele notaris zich wendt tot een externe dienstverlener om een specifiek AI-systeem te ontwikkelen en leveren, zijn een voorzichtige keuze van de aanbieder (due diligence wordt aanbevolen) en de afstemming van individuele contractuele voorwaarden voor AI-as-a-Service van cruciaal belang.
- De gebruiker moet duidelijk bepalen en in detail communiceren wat het precieze doel is van het systeem dat ontwikkeld moet worden en wat de kenmerken zijn, alsmede de regelgeving rondom de activiteit waarin het AI-systeem de gebruiker gaat assisteren.
- Er moet onderhandeld worden over een aantal belangrijke contractuele clausules met betrekking tot onder andere de gebruikte gegevensbronnen, de aansprakelijkheid van de aanbieder, de rechten op verschillende soorten gegevens, evenals op bescherming van persoonsgegevens en het regelmatig bijwerken en onderhouden van het systeem.
- Indien de notariële organisatie opdracht geeft tot extern geleverde AI-oplossingen (die vallen onder de materiële werkingssfeer van de AI Act) aan haar aangesloten notarissen—om de kwalificatie als aanbieder te omzeilen—moet de naam en/of het handelsmerk van de externe aanbieder worden vermeld in plaats van de naam van de notariële organisatie.

XIII. Basics of AI cybersecurity

1. Algemene inzichten

AI-technologie wordt steeds vaker gebruikt ter ondersteuning van de cyberbeveiliging van verschillende entiteiten ('*cyberveiligheid met AI*'). Tegelijkertijd worden AI-systemen zelf blootgesteld aan cyberaanvallen, waartegen bescherming in verschillende opzichten cruciaal is ('*cyberveiligheid van AI*'). Cyberaanvallen tegen AI-systemen kunnen niet alleen de werking van het gegeven systeem aantasten, maar kunnen ook verdere schade toebrengen aan de organisatie die ze gebruikt, variërend van negatieve reputatieschade tot inbreuken op de gegevensbescherming en ernstige financiële gevolgen.

Cyberbedreigingen en -aanvallen zijn opzettelijk en maken vaak gebruik van de kwetsbaarheden van de AI-systemen, voornamelijk gericht op de trainingsdata en de integriteit van het toegepaste algoritme. Door deze mogelijk aangetaste onderdelen kunnen aangevallen systemen gebruikt worden voor kwaadaardige doeleinden. Het belangrijkste doel van AI-cyberveiligheid is het voorkomen van onbevoegde toegang tot en manipulatie en misbruik van AI-systemen, met een focus op de beveiliging van gegevens en de bescherming van modellen. Als AI-systemen krachtiger worden en op grotere schaal worden gebruikt, wordt het behoud van hun robuustheid en veiligheid nog belangrijker.

In de volgende punten worden de mogelijkheden van cyberveiligheid met AI niet besproken; alleen de mogelijke cyberbedreigingen en aanvallen en de mogelijke maatregelen om dergelijke bedreigingen/aanvallen aan te pakken en de veilige werking van dergelijke systemen te waarborgen worden gepresenteerd. Het doel hier is om een basisinzicht te geven in de cyberveiligheid van AI voor notarissen. Technische details bespreken we daarom niet.

2. Beveiligingsrisico's voor AI-systemen en mogelijke tegenmaatregelen

Ter illustratie van hun uiteenlopende aard en zonder volledig te zijn, worden in de volgende subpunten enkele cyberbedreigingen en aanvallen op AI-systemen beschre-

ven. Ze kunnen invloed hebben op zowel de ontwikkelingsfasen (trainen, testen) als de uitrol (invoeren van prompts, leveren van output). Ze kunnen betrekking hebben op de integriteit [subpunten a)-d)], op de vertrouwelijkheid [subpunt e)] of op de beschikbaarheid van het AI-systeem [subpunt f)].

a) Ontwikingsaanvallen

In het geval van ontwikkelingsaanvallen—door gebruik te maken van de kwetsbaarheden van het model—manipuleren de aanvallers de input op een subtiele manier die resulteert in onjuiste output.

Bijvoorbeeld in het geval van beeldherkenning of gezichtsherkenning kan de ingevoerde afbeelding lichtjes gewijzigd worden op een manier die onwaarneembaar is voor het menselijk oog, waardoor het leidt tot een valse output (bv. vals positief voor de herkenning van het gezicht van de cliënt via videobellen). Vanuit technologisch oogpunt is het mogelijk om ontwikkelingsaanvallen aan te pakken, bijvoorbeeld door gebruik te maken van zogeheten *adversarial training*, waarbij het AI-model wordt blootgesteld aan en getraind op verschillende gemanipuleerde inputs. Daarnaast kan het continu controleren en analyseren van de inputs en outputs helpen bij het tegengaan van dergelijke aanvallen.

b) Training data poisoning

In het geval van training data poisoning worden kwaadaardige gegevens (bv. valse informatie, zoals verouderde wetteksten in plaats van de teksten die momenteel van kracht zijn) in de trainingsdataset van het AI-model gestopt. Data poisoning kan ook worden bereikt door (een deel van) de dataset te wijzigen of verwijderen. Het gevolg van data poisoning is een aangetast AI-model met een onvoorspelbare werking en onbetrouwbare en onnauwkeurige output. Deze aanval is bijzonder gevaarlijk, omdat de 'vergiftigde' gegevens vaak niet snel te identificeren zijn tussen de grote hoeveelheden trainingsdata. Wanneer een dergelijke inbreuk wordt gedetecteerd, moet deze worden getraceerd en moet de dataset onmiddellijk worden hersteld. In sommige gevallen moet het model volledig opnieuw worden getraind.

c) Model poisoning

Bij model poisoning wijzigen de aanvallers de modelparameters of de architectuur met kwade bedoelingen. Model poisoning wijzigt het gedrag van het model op een onverwachte manier. Het opsporen van modelvergiftiging is moeilijk omdat het vaak onmerkbaar is en de effecten alleen onder specifieke omstandigheden aan het licht komen.

Om dergelijke aanvallen aan te pakken wordt inspectie en opschoning van het model toegepast, waarbij het getrainde model wordt gecontroleerd op afwijkingen. Verder kan het model worden bijgesteld door fine-tuning, hertraining of het verwijderen van enkele parameters (snoeien).

d) Prompt injection

Prompt injection is specifiek voor LLM's, vooral bij natuurlijke taalverwerking (NLP). Prompt injection-aanvallen bestaan uit het maken van prompts om het gedrag van het AI-systeem te manipuleren, wat resulteert in de productie van schadelijke (bijv. vooringenomen of onnauwkeurige) of onbedoelde (onthulling van vertrouwelijke gegevens) output op basis van de afhankelijkheid van het systeem op die prompts. Deze aanvallen maken gebruik van het feit dat de output van een AI-model aanzienlijk kan worden beïnvloed door de formulering en structuur van de ingevoerde prompt.

Bij een chatbot kan de aanvaller bijvoorbeeld interacties van andere gebruikers met het systeem onderscheppen en goed ontworpen schadelijke prompts injecteren die vragen naar alle input van deze gebruikers (mogelijk inclusief vertrouwelijke gegevens).

Er zijn verschillende methoden beschikbaar om prompt injection-aanvallen tegen te gaan. Input kan bijvoorbeeld worden gezuiverd door het opschonen en valideren van prompts die AI-systemen ontvangen om ervoor te zorgen dat ze geen schadelijke inhoud bevatten (d.w.z. met behulp van reguliere expressies om input te identificeren en te blokkeren die overeenkomt met bekende schadelijke patronen). Daarnaast kan *adversarial training* (hierboven genoemd) ook nuttig zijn om prompt injection aanvallen tegen te gaan.

e) Modeldiefstal (modelextractie)

Modeldiefstal (of modelextractie) is het ongeautoriseerd (bijv. zonder toestemming van de ontwikkelaar) kopiëren van een AI-model. Dit kan worden beschouwd als een schending van intellectueel eigendom met aanzienlijke financiële gevolgen (door de waarde en kosten van de training van AI-modellen). Modeldiefstal brengt ook veiligheidsrisico's met zich mee, omdat het kan worden gebruikt om kwetsbaarheden te vinden voor verdere aanvallen.

AI-modellen beveiligen tegen diefstal houdt onder andere in dat er toegangscontroles worden ingevoerd (alleen geautoriseerde gebruikers kunnen interacteren met het model op basis van verificatie van gebruikersidentiteiten), versleuteling van de gegevens van het model en onzichtbare watermerken in outputs (om ongeoorloofd gebruik te traceren en te identificeren).

f) Denial-of-service (DoS)

Denial-of-service (DoS)-aanvallen zijn kwaadwillige pogingen om het functioneren van een AI-systeem te verstoren door het te overweldigen (door een buitensporige hoeveelheid prompts of complexe gegevensinvoer), waardoor het niet meer reageert of aanzienlijk trager wordt. Door de werking van het AI-systeem op een dergelijke manier te verstoren, krijgen legitieme gebruikers er geen toegang toe.

Dergelijke aanvallen kunnen worden tegengegaan door de robuustheid van het systeem te vergroten, bijvoorbeeld door ongebruikelijke verkeerspatronen te monitoren en door systemen te ontwikkelen die een plotselinge toename van prompts blokkeren.

3. Europese regelgeving voor AI-cyberveiligheid

a) Regelgevingslandschap

Ondanks het duidelijke belang van de cyberveiligheid van AI-systemen en het bestaan van algemene wetgeving op het gebied van cyberveiligheid (zoals de NIS2-richtlijn) op EU-niveau, bevat de huidige EU-wetgeving geen speciale rechtshandelingen met betrekking tot AI-cyberveiligheid, en andere rechtshandelingen (bijv. de AI Act) bevatten nauwelijks specifieke regels voor dit onderwerp. Er moet echter altijd rekening worden gehouden met nationale

wetgeving en zachte wetgeving op het gebied van (AI) cyberveiligheid (Nederland is bijvoorbeeld al begonnen met het opstellen van een plan voor cyberveiligheid—Het Nederlands Strategisch Actieplan voor AI—waarin relevante bepalingen zijn opgenomen).

b) AI Act

De AI Act bevat specifieke verplichtingen op het gebied van cybersecurity en robuustheid voor aanbieders met betrekking tot AI-systemen met een hoog risico (en AI-modellen voor algemene doeleinden met systeemrisico). De relevante artikelen (artikel 15) en overwegingen (66, 74 en 75) geven geen gedetailleerde richtlijnen over hoe aan deze verplichtingen moet worden voldaan.

In overeenstemming met artikel 15, lid 1, van de AI Act, *‘moeten AI-systemen met een hoog risico op zodanige wijze worden ontworpen en ontwikkeld dat zij een passend niveau van nauwkeurigheid, robuustheid en cyberveiligheid bereiken en dat zij gedurende hun gehele levenscyclus in die opzichten consistent presteren.’*

Bovendien wordt in lid 2 van hetzelfde artikel gesteld dat *AI-systemen met een hoog risico zo veerkrachtig mogelijk moeten zijn met betrekking tot fouten, storingen of inconsistenties die zich kunnen voordoen binnen het systeem of de omgeving waarin het systeem functioneert, met name door hun interactie met natuurlijke personen of andere systemen. In dit verband moeten technische en organisatorische maatregelen worden genomen.’*

Tot slot staat in lid 5 van artikel 15 dat *AI-systemen met een hoog risico weerbaar moeten zijn tegen pogingen van niet-geautoriseerde derden om het gebruik, de output of de prestaties ervan te wijzigen door misbruik te maken van kwetsbaarheden van het systeem. De technische oplossingen om de cyberveiligheid van AI-systemen met een hoog risico te waarborgen moeten zijn afgestemd op de relevante omstandigheden en risico's. De technische oplossingen om AI-specifieke kwetsbaarheden aan te pakken moeten, waar van toepassing, maatregelen bevatten om aanvallen te voorkomen, op te sporen, erop te reageren, op te lossen en te beheersen die proberen de trainingsdataset (data poisoning of vooraf getrainde componenten die worden gebruikt in training (model poisoning), ingangen die zijn ontworpen om het AI-model een fout te laten maken (tegengestelde voorbeelden of modelontwikking), aanvallen op vertrouwelijkheid of modelgebreken.’*

Alinea (4) kan zo worden opgevat dat de eis van robuustheid ook betrekking heeft op de veerkracht van AI-systemen tegen cyberaanvallen en ervoor zorgt dat een AI-systeem goed kan functioneren onder moeilijke omstandigheden (bijvoorbeeld wanneer het wordt blootgesteld aan cyberaanvallen).

Zelfs als artikel 15 en de bijbehorende overwegingen alleen van toepassing zijn op AI-systemen met een hoog risico moet, om het positieve imago van en het vertrouwen in het notariaat te behouden, de rechtszekerheid te waarborgen en de naleving van algemene (EU en mogelijk nationale) cyberveiligheidsverplichtingen te garanderen, ook bij de ontwikkeling en het gebruik van notariële AI-systemen die niet onder de categorie hoog risico vallen een hoog niveau van cyberveiligheid worden gewaarborgd.

c) AVG

Naast de AI Act bevat de AVG bepalingen die ook van toepassing kunnen zijn in de context van AI-cyberveiligheid, ondanks dat de AVG geen expliciete regels voor AI-systemen bevat. Deze regels hebben betrekking op verplichtingen rondom de beveiliging van (persoons)gegevens. Artikel 32 van de AVG bevat bepalingen over de beveiliging van de verwerking van persoonsgegevens voor verwerkingsverantwoordelijken en verwerkers door passende technische en organisatorische maatregelen te treffen om een toereikend beveiligingsniveau te waarborgen. Deze maatregelen bieden bescherming tegen verlies, wijziging, openbaarmaking en toegang. Hetzelfde artikel bevat een niet-uitputtende lijst van deze maatregelen (bijv. het waarborgen van de beveiliging van de verwerking) zonder verdere details te verstrekken. Aangezien de AVG een technologie-neutrale regeling is, moeten deze maatregelen met betrekking tot AI worden bepaald door per geval door onder andere rekening te houden met de potentiële risico's, kenmerken, doeleinden en de significantie van de betreffende AI-oplossing.

Met betrekking tot de technische en organisatorische controles moet Artikel 25 (1) van de AVG in aanmerking worden genomen, omdat in het kader van de vereiste van *‘gegevensbescherming door ontwerp’* de veilige verwerking van persoonsgegevens moet worden gegarandeerd. Deze regel heeft alleen betrekking op de verwerkingsverantwoordelijken.

Als een notariaat dus AI-systemen ontwikkelt die persoonsgegevens verwerken en/of de notarissen gebruiken

AI-systemen die dergelijke gegevens verwerken, moeten de bovenstaande regels van de AVG in aanmerking worden genomen.

Ten slotte moet de rol van standaarden met betrekking tot AI-systemen worden genoemd. De ISO (Internationale Organisatie voor Standaardisatie) heeft samen met de IEC (Internationale Elektrotechnische Commissie) verschillende AI-specifieke normen gepubliceerd (bijv. ISO/IEC TR 27563 over de use cases voor de impact van beveiliging en privacy op AI). De meeste van deze normen zijn omgezet door het CEN (Europees Comité voor Standaardisatie) en CLC (Europees Comité voor Elektrotechnische Standaardisatie). Het raadplegen van deze normen wordt sterk aanbevolen.

4. AI-cyberveiligheid en het notariaat

In het notariaat moeten zowel notariële organisaties als individuele notarissen actief meewerken aan het waarborgen van de cyberveiligheid van AI-systemen die door hen worden ontwikkeld/gebruikt.

De belangrijkste taak van de eerste is het ontwikkelen van dergelijke systemen die bestand zijn tegen aanvallen en om hun notarissen instructies en begeleiding te geven voor het juiste en veilige gebruik van dergelijke systemen. Vervolgens controleren, auditen en actualiseren ze deze systemen voortdurend zodat ze veerkrachtig genoeg zijn. Bovendien moeten notariële organisaties een strikte toegangscontrole instellen om te garanderen dat alleen de bevoegde personen de benodigde toestemmingen krijgen.

Notarissen moeten de verstrekte instructies en richtlijnen opvolgen, en als ze cyberbedreigingen of aanvallen detecteren, onmiddellijk de notariële organisatie waartoe ze behoren op de hoogte stellen om snel stappen te ondernemen om deze bedreigingen/aanvallen te voorkomen/tegen te gaan of om de negatieve gevolgen ervan te verhelpen.

Bij gebruik van AI-systemen ontwikkeld door externe dienstverleners moeten, naast de hierboven vermelde verplichtingen, de relevante contractvoorwaarden gedetailleerde bepalingen bevatten voor het waarborgen van toereikende cyberveiligheid. Het is cruciaal dat er notariële IT-experts betrokken zijn bij het opstellen van dergelijke contractvoorwaarden. Bovendien is het in elk geval raadzaam om externe specialisten op het gebied van cyberveiligheid te raadplegen.

Belangrijkste conclusies

- AI-systemen staan zelf bloot aan cyberaanvallen, waartegen bescherming van cruciaal belang is.
- Cyberbedreigingen en -aanvallen zijn opzettelijk en maken vaak gebruik van de kwetsbaarheden van de AI-systemen, voornamelijk gericht op de trainingsdata en de integriteit van het toegepaste algoritme.
- Cyberbedreigingen en aanvallen kunnen invloed hebben op zowel de ontwikkelingsfasen (trainen, testen) en de uitrol (invoeren van prompts, leveren van output). Ze kunnen doelgericht zijn en de integriteit, vertrouwelijkheid of beschikbaarheid van het AI-systeem aantasten.
- In dit hoofdstuk worden de ontwijkingsaanvallen, training data poisoning, model poisoning, prompt injection, modeldiefstal (modelextractie) en denial-of-service-aanvallen kort gepresenteerd, samen met mogelijke oplossingsmaatregelen.
- Momenteel zijn er geen specifieke rechtshandelingen op EU-niveau inzake AI-cyberveiligheid, en andere bestaande rechtshandelingen (bijv. de AI Act) bevatten nauwelijks bepalingen op dit gebied. Nationale wetgeving en zachte wetgeving moeten echter altijd worden gecontroleerd.
- De AI Act bevat specifieke verplichtingen op het gebied van cyberveiligheid en robuustheid

voor providers met betrekking tot AI-systemen met een hoog risico en AI-modellen voor algemene doeleinden met systeemrisico, zonder gedetailleerde richtlijnen te geven over hoe aan deze verplichtingen voldaan moet worden.

- Ook in het geval van notariële AI-oplossingen die niet onder de categorie hoog risico vallen wordt een hoog niveau van cyberveiligheid aanbevolen.
- Artikel 32 van de AVG bevat bepalingen over de beveiliging van de verwerking van persoonsgegevens voor verwerkingsverantwoordelijken en verwerkers door passende technische en organisatorische maatregelen te treffen en artikel 25 van dezelfde wet ('gegevensbescherming door ontwerp') wordt ook toegepast in de context van AI-cyberveiligheid.
- Het raadplegen de relevante internationale en Europese normen wordt sterk aanbevolen.
- Zowel notariële organisaties als individuele notarissen moeten actief meewerken aan het waarborgen van de cyberveiligheid van AI-systemen die door hen worden ontwikkeld/gebruikt.
- Bij gebruik van AI-systemen ontwikkeld door externe dienstverleners moeten de toepasselijke contractuele voorwaarden gedetailleerde bepalingen bevatten om een toereikende cyberveiligheid te waarborgen.
- Het is in elk geval sterk aan te raden om externe specialisten op het gebied van cyberveiligheid te raadplegen.

Uitgever:

Raad van de Notariaten van de Europese Unie (CNUE)
B-1000 Bruxelles - Avenue de Cortenbergh, 120
T. +32 2 513 95 29
info@cnue.be
www.notariesofeurope.eu

Auteur:

Tamás Sajben

Bijdragers:

Leden van het CNUE Futurology Forum, de New Technologies Working Group en de Data Protection Task Force

Jaar van publicatie:

2025

Afbeelding omslag: AI-chatbot is het proces van kunstmatige intelligentie tussen systemen en mensen. Met andere woorden, een AI-chatbot is een virtuele klantenservice die actief kan communiceren met de gebruikers. Foto door KhunkornStudio. Achtergrondfoto: Concept art van cloud-opslag van digitale gegevens. Foto door Keopaserth.