SIRIUS.LEGAL
BUSINESS LAW FIRM

ARTIFICIËLE INTELLIGENTIE IN MARKETING: OOK VOOR DE KMO

MET WELKE LEGALE ASPECTEN MOET JE REKENING HOUDEN?

Inhoud

Juridische aandachtspunten in AI-trajecten

door Bart Van den Brande, Managing partner, Sirius Legal Business Law Firm

Alexa, Siri en de Google Assistent, zelfrijdende wagens, spraak- en gezichtsherkenning, beeld- en tekstanalyse software, … Artificiële Intelligentie is de voorbije jaren aan een ware explosie bezig en bewust of onbewust wordt het leven van élk van ons vandaag al dagelijks beïnvloed door (de gevolgen van) AI: van de reclame die we te zien krijgen, tot de regeling van de verkeerslichten waar we staan te wachten terwijl we die reclame wegswipen op onze smartphone.

Kunstmatige intelligentie wordt dan ook terecht door de EU beschouwd als één van de essentiële bouwstenen voor de digitale maatschappij van de toekomst. Gelet op de snelheid waarmee de rekenkracht van computersystemen evolueert is die toekomst niet morgen, maar gisteren al begonnen.

AI-toepassingen brengen ook een hele reeks juridische en ethische uitdagingen met zich mee. Inmiddels zijn er al boeken volgeschreven met juridische analyses over de impact van AI op bestaande wetgeving of omgekeerd.

Als we de dingen zeer pragmatisch bekijken, kunnen we echter de grote uitdagingen voor ondernemers die in aanraking komen met AI, terugbrengen tot een viertal clusters, die we hieronder zullen behandelen:

- Specifieke (toekomstige) regelgeving over de manier waarop AI-tools ingezet kunnen en mogen worden;
- Cyber security en de veiligheid van data in AI-toepassingen;
- Correct omgaan met persoonsgegevens onder GDPR binnen AI-toepassingen;
- Intellectuele eigendomsrechten op AI én op wat AI-toepassingen voortbrengen.

We geven je hieronder géén uitgebreide juridische analyse, daar ben je als ondernemer weinig mee. We proberen je wel een overzicht te geven van de regels waar je rekening mee moet houden én een overzicht van praktische aandachtspunten. Dat overzicht kan je bij wijze van checklist in het achterhoofd houden.

De toekomstige EU-regels voor de ontwikkeling en het gebruik van Artificiële Intelligentie of Machine Learning

Eerste poging in de wereld om AI te reguleren

De razendsnelle evolutie die we hierboven al beschreven, heeft de voorbije jaren het besef doen groeien dat er dringend nood is aan een regelgevend kader voor artificiële intelligentie. In het beste geval maakt AI of Machine Learning ons leven aangenamer, maar als diezelfde technologie in verkeerde handen zou komen, kan dat potentieel desastreuze gevolgen hebben, bijvoorbeeld voor jouw en mijn privacy.

Precies om die reden wordt er achter de schermen binnen de EU al 2 jaar gewerkt aan een regelgevend kader dat moet zorgen voor een veilig en ethisch verantwoord gebruik van AI binnen de EU. Eind april 2021 maakte de Europese Commissie een eerste ontwerp publiek van een "AI Verordening"[1] die hieruit voort zou moeten vloeien. Dit ontwerp is wereldwijd de allereerste echte poging om een wetgevend kader voor AI te creëren. De EU wil immers een voorloper zijn in nieuwe technologie en digitalisering.

"Risk based approach" die doet denken aan GDPR

De nieuwe regels doen bij een eerste lezing onmiddellijk denken aan de GDPR, die sinds 2018 in de EU en tot ver daarbuiten bepaalt hoe bedrijven mogen omgaan met jouw en mijn persoonsgegevens. Op een gelijkaardige manier wil de EU voor het volledige grondgebied van de EU op één en dezelfde wijze reguleren hoe bedrijven data (al dan niet persoonsgegevens) kunnen inzetten binnen AI-algoritmes.

Eén van die opvallende raakpunten met de aanpak onder GDPR is de zogenaamde "risk based approach": AI-development zal een risicoanalyse vereisen en AI-systemen die een duidelijke bedreiging vormen voor de veiligheid en rechten van Europese burgers, worden eenvoudigweg verboden. Het gaat dan om AI-toepassingen die menselijk gedrag manipuleren of de vrije wil van betrokkenen (personen wiens gegevens verwerkt worden) omzeilen. De Europese Commissie geeft zelf als voorbeeld "smart" speelgoed met spraaktechnologie dat kinderen kan aansporen tot gevaarlijk gedrag. De Commissie maakt een onderscheid tussen "hoog risico" AI, "beperkt risico" AI en "minimaal risico" AI.

Hoogrisico AI-systemen zijn systemen die gebruikt worden voor publieke infrastructuur (bv. verkeer), in medische omgevingen, in het kader van beroepsopleidingen of toegang tot onderwijs (bv. verbeteren van examens), werkgelegenheid, personeelsbeleid (bv. screening bij sollicitaties), essentiële diensten zoals bank- en kredietdiensten (kredietwaardigheidschecks), gebruik door politiediensten, douanediensten, rechtbanken en andere overheden (inclusief bijvoorbeeld ook alle mogelijke biometrische systemen van gezichtsherkenning, stemherkenning, vingerafdrukherkenning, etc…).

1 https://ec.europa.eu/commission/presscorner/detail/nl/ip_21_1682

Deze toepassingen zullen aan strenge verplichtingen worden onderworpen voordat zij in de handel mogen worden gebracht:

- Ondernemingen zullen een voorafgaande risico-audit moeten doorlopen, vergelijkbaar met de Gegevensbeschermingeffectenbeoordeling of Data Protection Impact Assessment die vandaag al bestaat onder GDPR;
- Op basis van die risico-audit zullen zij de nodige maatregelen moeten nemen om de impact op de gebruiker te minimaliseren;
- Ondernemingen zullen moeten zorgen voor datasets van hoge kwaliteit om risico's op bijvoorbeeld discriminerende resultaten zoveel mogelijk uit te sluiten;
- Er zal een registratieplicht (!) gelden voor heel wat AI-toepassingen;
- Ondernemingen zullen gedetailleerde documentatie en transparantie moeten voorzien naar de overheid over de werking van hun algoritmes;
- Transparante informatie voor betrokkenen is een basisplicht, net zoals onder GDPR;
- Ondernemingen zullen moeten zorgen voor gepaste menselijke controle en toezicht op hun AI--toepassingen;
- (cyber-)Veiligheid, robuustheid en nauwkeurigheid zijn bijna vanzelfsprekende noodzakelijkheden. Op cyber security komen we overigens verderop in deze tekst nog afzonderlijk terug.

Classificatiemodel

We gaven al aan dat Europa een indeling voorziet van AI-toepassingen in verschillende categorieën, afhankelijk van de potentiële impact die ze kunnen hebben op de betrokkenen. Zo maakt men een onderscheid tussen artificiële intelligentie met een onaanvaardbaar risico, die sowieso verboden zijn, toepassingen met een hoog risico, toepassingen met een beperkt risico en toepassingen met een minimaal risico.

Sommige AI-toepassingen zijn dus per definitie verboden. Dat is bijvoorbeeld het geval voor toepassingen die erop gericht zijn om de zwakheden van mensen uit te buiten om hun gedrag te manipuleren, zeker als het daarbij gaat om zwakkere groepen in de maatschappij zoals jongeren, bejaarden, mensen met een fysieke of mentale handicap.

Andere AI-toepassingen worden als "hoog risico" beschouwd. Systemen voor biometrische identificatie op afstand bijvoorbeeld, zijn enkel toegelaten als ze aan strikte eisen voldoen. Dat soort toepassingen kan bijvoorbeeld (en behoudens uitzonderingen) niet gebruikt worden door politiediensten of overheden op openbare plaatsen. Een typisch voorbeeld is gezichtsherkenning via publieke camera's. Ook AI-toepassingen in het onderwijs, in kritieke economische sectoren, in de context van werkgelegenheid en personeelsbeleid en die impact hebben op fysieke veiligheid van personen (bv. AI in chirurgische toestellen) worden per definitie als hoog risico beschouwd.

Onder AI-toepassingen met beperkt risico verstaat de Verordening bijvoorbeeld chatbottoepassingen. Hier is het vooral zaak om de gebruiker transparant en correct te informeren over het gebruik van AI, zodat hij of zij zelf kan beslissen om wel of niet met een softwaretoepassing in gesprek te gaan.

De laatste categorie is met voorsprong de grootste. Het gaat om duizenden AI-toepassingen voor dagelijks gebruik, die slechts een "minimaal risico" met zich meebrengen. Als voorbeelden worden vernoemd: "slimme" spamfilters, zelflerende videogames, predictieve marketingtools, slimme keukentoestellen, … De ontwerpverordening laat die systemen ongemoeid aangezien het risico voor de rechten of de veiligheid van burgers minimaal of onbestaand is (wat overigens niet betekent dat andere regels, zoals precies GDPR, niet van kracht zouden kunnen zijn op deze toepassingen, natuurlijk).

Wat moet ik intussen en in afwachting van die verordening concreet als ondernemer doen?

Zolang de aangekondigde AI-verordening niet definitief is, kan je ze als ondernemer natuurlijk moeilijk toepassen. Inhoudelijk kan er nog heel wat veranderen en de precieze uitwerking van heel wat elementen is nog onduidelijk of onvoldoende gedetailleerd.

Dat neemt echter niet weg dat vooruitziende ondernemers alvast de basisbeginselen kunnen integreren in hun AI-traject. De aanzet tot die basisbeginselen zit al in het ontwerp van verordening vervat. De precieze uitwerking is nog niet helemaal duidelijk, maar aangezien het gaat om beginselen die erg gelijkaardig zijn aan verplichtingen die ook al bestaan onder GDPR of principes uit consumentenbescherming, is het niet moeilijk om een concrete invulling te geven die alvast de geest van de toekomstige wetgeving respecteert.

Wat kan je concreet alvast doen vandaag?

- Zorg vooraf voor een impact assessment:
    - » Vertrek vanuit de principes van een DPIA of GBEB[2] onder GDPR en combineer beide oefeningen waar mogelijk in 1 document;
    - » Documenteer de inhoudelijke werking van je toepassing;
        - » Welke gegevens worden erin verwerkt (en gaat het al dan niet om persoonsgegevens, bedrijfskritische gegevens, vertrouwelijke knowhow voor het bedrijf, ...)?;
        - » Met welk doel worden die gegevens erin verwerkt?;
        - » Beschrijf ook de onderliggende logica / gevolgtrekkingen en afgeleide data / Machine Learning aspecten;
        - » Is aan de voorgenomen verwerking enige gevoeligheid verbonden of enige te verwachten impact op de betrokken personen?;
        - » Kan je transparantie garanderen naar betrokkenen toe?;
    - » Identificeer risico's voor de betrokkenen (inbreuken op privacy, inbreuken op GDPR, potentiële impact op privéleven, beperking van toegang tot bepaalde goederen of diensten, …);
    - » Tracht de vastgestelde risico's te vermijden of op zijn minst te minimaliseren door middel van daartoe "gepaste" maatregelen die je in je impact assessment beschrijft;
    - » Zorg voor een vervolgtraject waarin het wegwerken of de minimalisering van de vastgestelde risico's effectief geïmplementeerd wordt;

2 Data Protection Impact Assessment of Gegevensbeschermingseffectbeoordeling

- Zorg voor transparante informatie naar de betrokkenen toe (noteer dat, in geval van verwerking van persoonsgegevens onder GDPR, sowieso uitgebreide transparantie over deze en andere punten verschaft moet worden):
    - » Identiteit van je bedrijf en mogelijkheid om contact te nemen;
    - » Doel van de toepassing;
    - » Verwerkte gegevens;
    - » Onderliggende basislogica;
    - » Partijen met wie data gedeeld wordt;
    - » Potentiële risico's;
    - » Maatregelen die genomen zijn om risico's te vermijden of te beperken;
    - » Desgevallend verplichte transparantie volgend uit de toepassing van GDPR (bewaartermijnen, rechten van de betrokkene, profiling, automatische beslissingsname, gegevensexport buiten de EER, identiteit van verwerkers, …).

Bedrijven die op die manier al proactief inspelen op deze toekomstige verordening, geven zichzelf in zekere zin een voorsprong. Wie bewust en actief stilstaat bij de opbouw en de impact van zijn of haar AI-toepassing, versterkt zijn toepassing, versterkt zijn merk en imago ook, minimaliseert het risico op klachten of negatieve feedback en werkt in het algemeen aan een ethisch, betrouwbaar en imagoversterkend kader voor artificiële intelligentie binnen zijn of haar onderneming.

Bescherming van persoonsgegevens en GDPR

Machine Learning en AI vragen door hun aard om grote hoeveelheden beschikbare data en vrije datastromen. Van zodra die data echter persoonsgegevens onder GDPR blijken te zijn, gaan er voor bedrijven en organisaties binnen de EU heel wat knipperlichtjes af. GDPR brengt immers een hele reeks verplichtingen en beperkingen met zich mee in de manier waarop omgegaan mag worden met persoonsgegevens. Die regels leggen al snel heel wat beperkingen op waar je rekening mee moet houden in AI-trajecten.

We sommen hieronder de belangrijkste aandachtspunten op en geven je daarna ook enkele duidelijke aanknopingspunten om één en ander vervolgens praktisch op te vangen binnen een AI- of Machine Learning project.

Data Protection by Design en by Default

AI-toepassingen moeten in de EU rekening houden met heel wat verplichtingen uit de GDPR.

Software en algoritmes die gebaseerd zijn op Artificiële Intelligentie of Machine Learning zullen bijvoorbeeld "Data Protection by Design" en "Data Protection by Default" moeten zijn. Dat betekent dat ondernemingen vanaf de eerste stappen in de ontwikkeling of de implementatie van (AI of andere) software tools, alle nodige technische en organisatorische maatregelen moeten inbouwen die nodig zijn om de basisbeginselen en de "rechten van de betrokkene" uit de GDPR vanaf het prille begin te waarborgen.

Niet enkel wie AI-toepassingen ontwikkelt, is overigens gebonden door bovenstaande beginselen. Ook wie software wil aankopen of op maat wil laten ontwikkelingen door een softwareleverancier of developer, moet rekening houden met Data Protection by Design en by Default en moet dit meenemen in zijn of haar beslissingsproces bij de keuze voor de ene of de andere partner. 'Wie kan de beste privacygaranties bieden' wordt met andere woorden een belangrijke factor in élk digitaal aankoop- of ontwikkelingstraject.

De noodzaak om te zorgen voor de nodige privacywaarborgen in het design zelf van de toepassing, zorgt voor heel wat uitdagingen in de context van AI en Machine Learning. De basisbeginselen uit de GDPR bijvoorbeeld zeggen dat data in alle transparantie verwerkt moeten worden en dat betrokkenen het recht hebben om te weten welke persoonsgegevens over hen (machinaal) verwerkt worden, om zich in bepaalde gevallen te verzetten tegen zulke verwerking, om de verbetering en soms ook de verwijdering van hun data te vragen of om de toestemming die ze in het verleden misschien gegeven hebben, in te trekken. GDPR voorziet zelfs in een specifieke bescherming van de betrokkene bij de verwerking van persoonsgegevens in het kader van profilering en met het oog op "geautomatiseerde beslissingsname", precies twee typische toepassingsgebieden van AI.

In al die gevallen moet de "verantwoordelijke voor de verwerking" (lees: de eigenaar van de data) kunnen garanderen dat die rechten ook correct, precies en tijdig (binnen 30 dagen) nageleefd worden.

Maar precies daar wil het weleens fout gaan met AI-toepassingen. Vaak zijn data niet zomaar verwijderbaar of verbeterbaar en in heel wat gevallen is het zelfs onduidelijk wélke data precies binnen een zelflerende softwaretoepassing "verwerkt" worden. Heel wat "afgeleide" data zijn immers, ten minste voor zover ze nog teruggekoppeld kunnen worden aan een bepaalde persoon, ook als een persoonsgegeven te beschouwen, wat betekent dat AI-toepassingen heel wat data genereren, waarmee eveneens rekening gehouden moet worden. Die zelfgegenereerde data zijn bovendien vaak van belang voor de verdere toekomst van het machine learning proces en het geregeld verwijderen van data is dan potentieel erg nadelig voor het verdere ontwikkelingsproces van de toepassing.

Binnen GDPR spelen bovendien nog andere beginselen mee die absoluut gewaarborgd moeten zijn en die binnen de specifieke context van AI toch voor complicaties kunnen zorgen. Gegevensbeschermingswetgeving zegt bijvoorbeeld dat een verantwoordelijke enkel die data mag verzamelen die strikt noodzakelijk is om een bepaald doel te bereiken en dat data in se enkel gebruikt kan worden voor het specifieke doel waarvoor ze verzameld werden. Bovendien mogen persoonsgegevens niet langer bewaard worden dan noodzakelijk is en moeten ze daarna onherroepelijk verwijderd worden of op zijn minst (volledig en definitief) geanonimiseerd worden. Ook die basisbeginselen moeten absoluut gewaarborgd kunnen worden binnen een AI-traject.

Dataregister

Hou er ook rekening mee dat de absolute basis van alle oefeningen in GDPR compliance, zowel binnen AI-projecten als daarbuiten, de noodzaak is tot het aanleggen van een goed, volledig, gedetailleerd en up--to-date dataregister.

Hoe vollediger en gedetailleerder je dataregister is, hoe makkelijker het wordt om een aantal verplichtingen onder GDPR te garanderen:

- Je dataregister bevat alle basisinformatie die je toelaat om transparantieverplichtingen na te leven. Je privacy policy bijvoorbeeld, kan je enkel juist en volledig opstellen als je daarvoor je dataregister bij de hand kan pakken;
- In geval van datalekken is je dataregister de eerste hulpbron om de aard, omvang en impact van een lek in te schatten. Het helpt je om vast te stellen welke data gecompromitteerd zijn, waar die zich bevinden, wie er toegang tot heeft, met wie je ze deelt en alle andere nuttige info om snel en efficiënt te handelen;
- In al die gevallen waarin een DPIA nodig is, is je dataregister je eerste hulpbron, om dezelfde redenen als hierboven vermeld;
- En ook nog: bij eventuele controles door de overheid, om welke reden dan ook, zal de eerste vraag bijna automatisch zijn om het dataregister te mogen inkijken. Wie op dat ogenblik geen up to date dataregister heeft, staat voor een moeilijk gesprek.

Verwerkersovereenkomsten met alle partners

Verwerkt jouw AI-toepassing persoonsgegevens volgens de regels van de GDPR, en werk je voor de verzameling, of de verwerking van data samen met een of meer derde partijen die in het kader van hun opdracht toegang krijgen tot jouw database met persoonsgegevens? Dan moet je met deze derden een zogenaamde “verwerkersovereenkomst” afsluiten.

In die verwerkersovereenkomst moet jouw partner je garanderen dat hij of zij in overeenstemming met alle verplichtingen van de GDPR, veilig, verantwoord én binnen de grenzen van de opdracht die jij geeft, met jouw persoonsgegevens zal omgaan.

Let op, het is jouw verantwoordelijkheid om ervoor te zorgen dat je de juiste, betrouwbare partners kiest én dat je met hen een gepaste verwerkersovereenkomst tekent. Als er geen verwerkersovereenkomst bestaat tussen jullie, kan jij, als “verantwoordelijke voor de verwerking”, een boete oplopen, die bijzonder hoog kan oplopen.

Waarop moet je specifiek letten vanuit AI-oogpunt in verwerkersovereenkomsten met partners in je automatiseringsproject?:

- Zorg voor een duidelijke omschrijving van de taken en bevoegdheden van de verwerker;
- Zorg voor een duidelijke omschrijving van de data waar je verwerker toegang toe zal krijgen én voor een duidelijke beschrijving van de data die desgevallend gegenereerd zal worden onder zijn of haar toezicht of binnen zijn of haar opdracht;
- Zorg voor een duidelijke oplijsting van de technische en organisatorische maatregelen waarvan jij verwacht dat je verwerker ze geïmplementeerd heeft om jouw data veilig te houden;
- Zorg voor transparantie over de identiteit van alle sub-verwerkers waar je verwerker beroep op doet;
- Zorg voor transparantie over eventuele data-export door jouw verwerker of door diens sub-verwerkers buiten de EU (of beter: de EER, dat is de EU uitgebreid met Ijsland, Noorwegen en Liechtenstein);
- Zorg voor duidelijke en strenge afspraken die absolute transparantie en medewerking garanderen in geval van (twijfel over eventuele) datalekken bij je verwerker;
- Zorg voor duidelijke en strenge aansprakelijkheidsclausules in jouw voordeel, die je toelaten om bijvoorbeeld bij datalekken eventuele kosten en schade op je verwerker te verhalen;
- Zorg voor duidelijke afspraken over (de kosten van) de medewerking van jouw verwerker bij eventuele Data Protection Impact Assessments die jij zou moeten uitvoeren als verantwoordelijke voor de verwerking (meer over DPIA's verderop in deze tekst).

Data Protection Officer

Hou er rekening mee dat je als gevolg van een AI-project misschien moet overgaan tot de aanstelling van een DPO of Data Protection Officer, als je dat eerder nog niet zou gedaan hebben. De Data Protection Officer is een persoon die binnen de onderneming verantwoordelijk is voor het toezien op de naleving van privacywetgeving. Hij of zij zal advies geven over nieuwe software, gebruik van database, etc. Hij of zij zal ook de contactpersoon ziijn bij de overheid in geval van bijvoorbeeld datalekken.

Niet elk bedrijf is verplicht om een DPO aan te stellen. Je hebt een DPO nodig in volgende gevallen:

- Je bedrijf of organisatie is een overheidsinstantie;
- Je verwerkt of monitort persoonsgegevens op grote schaal en met grote regelmaat;
- Je verwerkt bijzondere categorieën van gevoelige gegevens zoals ras, politieke voorkeur, religie of medische gegevens op grote schaal;
- Ook als je in opdracht van de federale overheid persoonsgegevens verwerkt, moet je in ieder geval een DPO aanstellen.

In veel gevallen is het nuttig voor (grotere) bedrijven die buiten deze categorieën vallen om toch een DPO aan te stellen. De DPO kan overigens een externe dienstverlener zijn. In de meeste gevallen is het zelfs aangeraden om hiervoor iemand extern in te schakelen om redenen van onafhankelijkheid van de persoon in kwestie, maar ook om aansprakelijkheidsredenen.

Specifiek in het kader van AI-toepassingen is vaak sprake van permanente of grootschalige monitoring en verwerking van persoonsgegevens. Wat precies als "grootschalig" beschouwd moet worden, is weliswaar nergens gedefinieerd, maar zodra er sprake is van regelmaat (bijvoorbeeld monitoring van aankopen in een supermarkt op basis van klantenkaarten, locatiegegevens van personeel), van grote hoeveelheden gegevens (uitgebreide datasets) of van gegevens over veel verschillende personen of zodra de verwerking over een groot grondgebied verspreid zit, is de kans groot dat een DPO verplicht is.

Bij twijfel of een DPO nodig is, neem je best geen risico. De aanstelling van een DPO is een verplichting onder de GDPR en het loutere feit dat geen DPO werd aangesteld waar dat wel nodig is op zich, is reden om zeer hoge boetes uit te keren.

Let ook goed op bij de keuze van je DPO. De GDPR voorziet immers een hele reeks vereisten en incompatibiliteiten omwille van interne belangenconflicten. Win tijdig advies in als je niet zeker bent van je zaak.

Data Protection Impact Assessments

Een Data Protection Impact Assessment of in het Nederlands: *"gegevensbeschermingseffectbeoordeling"* is een analyse die je voorafgaandelijk moet maken als je bepaalde verwerkingen van persoonsgegevens wil opstarten.

In een DPIA moet je een grondig voorafgaand onderzoek doen naar zowel de opportuniteit van de voorgenomen verwerking en het respect voor de rechten van de betrokkene als van de technische en organisatorische veiligheid van de voorgenomen verwerking. Je moet met andere woorden een voorafgaande inschatting maken van de impact die jij zal hebben op de privacy en de dataveiligheid van de betrokkenen wiens gegevens je gaat verwerken. Die voorafgaande analyse moet gedocumenteerd zijn. Als je onderweg risico's vaststelt, moet je ook beschrijven welke maatregelen je alsnog zal nemen om die risico's weg te nemen of te minimaliseren.

De Gegevensbeschermingsautoriteit voorziet een lijst met gevallen waarin zo een DPIA nodig is. In de context van AI-toepassingen voor KMO's gaat het vooral om (samengevat en bij wijze van voorbeeld) deze criteria:

- Je wil nieuwe technologie inzetten;
- Je wil grote hoeveelheden data verwerken;
- Je wil verschillende bestaande datasets aan elkaar koppelen;
- Je wil gegevens van zwakkere groepen in de maatschappij verwerken (minderjarigen, sociaal zwakkeren);
- Je wil "gevoelige" gegevens verwerken (bv. biometrische data, medische gegevens, gegevens over politieke voorkeuren, lidmaatschap vakbond, religieuze overtuiging, seksuele voorkeur, …);
- Ook het evalueren, profileren en scoren van personen vereist een voorafgaande DPIA
- ...

Elk van deze criteria op zichzelf geven niet noodzakelijk aanleiding tot de noodzaak aan een DPIA, de combinatie van 2 of meer van deze aspecten wél.

Het is de verantwoordelijke voor de verwerking die moet zorgen dat tijdig een DPIA wordt uitgevoerd. "Tijdig" betekent in deze context "voordat enig developmentwerk start en voordat de verwerking van persoonsgegevens begint". Heb je ook een Data Protection Officer of DPO aangesteld? In dat geval zal ook hij/zij advies moeten geven over deze Data Protection Impact Assessment.

Organisatorische en technische maatregelen.

Eén van de hoekstenen van GDPR is ook de verplichting om “gepaste technische en organisatorische maatregelen” te nemen om een “gepaster niveau van bescherming” voor persoonsgegevens te kunnen garanderen en dit zowel op het niveau van je AI-toepassing zelf, als in bredere context binnen je onderneming.

Als je op je AI-toepassing een DPIA uitgevoerd hebt, zoals besproken onder het voorgaande punt, dan zullen eventuele risico’s verbonden aan je AI-project zelf naar boven gekomen zijn en dan heb je in je DPIA omschreven welke “technische en organisatorische” maatregelen je gaat voorzien om die risico’s weg te nemen of te beperken.

Daarnaast zal je eenzelfde “veiligheidsoefening” ook breder in je onderneming moeten uitvoeren om in kaart te brengen of je veilig omspringt met persoonsgegevens, bijvoorbeeld in de context van thuiswerk, bij de uitwisseling van gegevens binnen of buiten je bedrijf, bij het opslaan en vernietigen van papieren documenten, bij het gebruik van e-mail en andere communicatietools, bij de (digitale) opslag van gegevens (on premise of in de cloud), ...

Typische voorbeelden van zulke technische en organisatorische maatregelen die in heel wat bedrijven toegepast kunnen worden, zijn:

- Versleuteling van databases;
- Paswoordbeheer of log-in beheer door bijvoorbeeld dubbele authenticatie;
- Document access management;
- Thuiswerk policies, bring-your-own-device policies, e-mail policies, bezoekers policies, …;
- Periodieke intrusietesten en veiligheidstesten op softwaresystemen;
- Gepaste technische beveiliging (antivirussoftware, firewall, etc…);
- Gepaste back-ups en garanties op datacontinuïteit,
- Interne opleidingen en awareness;
- ...

Data Export

Afgelopen zomer oordeelde het Europees Hof van Justitie in haar Schrems II-arrest dat het zogenaamde “Privacy Shield” dat de uitwisseling van persoonsgegevens van de EU naar de VS mogelijk maakte zonder bijkomende waarborgen of beperkingen in strijd was met het Europees recht en met name met GDPR. Premisse van het Privacy Shield was immers de “belofte” van Amerikaanse bedrijven dat de persoonsgegevens van Europese burgers eenzelfde niveau van veiligheid zouden genieten in de VS als in de EU en dat uitgangspunt is de facto onmogelijk. Amerikaanse veiligheidswetgeving, zoals bijvoorbeeld de FISA act, geven Amerikaanse inlichtingendiensten immers vergaande inzagerechten in (Europese of andere) datastromen die de VS binnenkomen. Europese data zijn dus nooit echt “veilig” in de VS en die vaststelling betekende meteen ook het einde van het Privacy Shield.

De gevolgen hiervan zijn potentieel érg vergaand. Quasi alle software tools die Europese bedrijven vandaag gebruiken en zéker ook heel wat AI-tools, zijn immers Amerikaans en aangezien de meeste daarvan tegenwoordig cloud services of online tools zijn, is er per definitie sprake van gegevensuitvoer naar de VS.

Het probleem werd enkel maar groter als we ook rekening houden met het feit dat het EHJ daar ook aan toevoegde dat wie data exporteert buiten de EU (ook naar andere bestemmingen dan de VS), meteen rekening moet houden met het feit dat de Standard Contract Clauses die de Europese Commissie zélf voorziet om veilige gegevensexport te garanderen tussen bedrijven en organisaties binnen en buiten de EU niet volstaan.

Het Schrems II-arrest zegt immers zeer duidelijk dat overdrachten van persoonsgegevens aan cloudservice providers in de Verenigde Staten geval per geval beoordeeld moeten worden en indien er een risico bestaat voor de integriteit van de betreffende gegevens, moeten bijkomende veiligheidswaarborgen voorzien worden. Die aanvullende waarborgen dringen zich bij export naar de VS bijna automatisch op, gelet op de zeer vergaande onderzoeksbevoegdheden van de Amerikaanse inlichtingendiensten, bijvoorbeeld op grond van sectie 702 (50 USC § 1881a) van de Foreign Intelligence Surveillance Act (Cloud Services Act).

Data export compliance is dan ook een zeer belangrijk onderdeel van elke AI-project. Je wil er immers zeker van zijn dat (idealerwijze) je data in Europa blijven of (desnoods) dat de eventuele export buiten de EU gebeurt volgens de regels van de juridische kunst, en mét de nodige bijkomende veiligheidsgaranties.

Wat moet je concreet doen?:

- **Stap 1**: maak een inventaris van alle gegevens die je exporteert naar derde landen. Als je al een dataregister hebt, is dit een eenvoudige stap voor jou en kan je ineens naar de volgende stap gaan. Klinkt het woord 'dataregister' Chinees voor jou, dan leggen we dit graag even uit. De GDPR legt aan elke verwerkingsverantwoordelijke de verplichting op om alle verwerkingsactiviteiten vast te leggen die onder haar verantwoordelijkheid plaatsvinden. Concreet breng je in zo'n dataregister een aantal zaken in kaart voor alle gegevens die je verzamelt: de doeleinden, de middelen, de rechtsgrond, de risico's voor de privacy van de betrokkenen, de toegang tot die gegevens, de doorgifte aan derden, … Zo krijg je een overzicht van alle datastromen binnen de onderneming. Dit vereenvoudigt de eventuele controles en audits aanzienlijk. Je kan hiervoor gebruikmaken van een aantal kwalitatieve vragenlijsten of evaluatietools, maar uiteraard kan Sirius legal je hierbij gespecialiseerde ondersteuning bieden.
- **Stap 2**: contacteer je dienstverleners/contractpartijen in het derde land. Je doet er goed aan om al je contractpartijen, dienstverleners en dergelijke te informeren over het Schrems-II arrest en de gevolgen hiervan. Sirius Legal heeft hiervoor een standaard brief template gemaakt met een Data Export Vendor Assessment. Je kan deze template gratis downloaden onderaan dit blogbericht. Met 'derde land' willen we niet elk ander land dan je eigen land zeggen, maar wel elk land dat buiten de Europese Economische Ruimte ligt, dat is de EU uitgebreid met Noorwegen, Ijsland en Liechtenstein.
- **Stap 3**: ga na of er een beslissing over een passend beschermingsniveau in het derde land is. Voor sommige derde landen heeft de Europese Commissie beslist dat dit land een passend beschermingsniveau biedt ('een adequaatheidsbesluit'), dus kan je de gegevensexport naar die landen op basis van die beslissing doen. De volledige lijst van die landen kan je op de website van de Europese Commissie vinden. Momenteel zijn er onderhandelingen bezig met Zuid-Korea. We volgen dit uiteraard op en houden je via onze blog en sociale media continu op de hoogte over eventuele wijzigingen.
- **Stap 4**: beoordeel de juridische situatie van het derde land. Wanneer er sprake is van gegevensexport naar een derde land waar geen beslissing over een passend beschermingsniveau is, dan komen we bij de volgende stap. De gegevensbeschermingsautoriteit van Baden-Württemberg raadt in dat geval aan om de juridische situatie van dat derde land grondig te onderzoeken. Het is in dit kader vooral interessant om na te gaan of nationale veiligheidsinstanties toegang kunnen krijgen tot de geëxporteerde gegevens. Je kan hiervoor ten rade gaan bij je nationale gegevensbeschermingsautoriteit (in België is dat de GBA, in Nederland de AP, in Frankrijk de CNIL en in Engeland de ICO), de Europese Commissie, de EDPB, het nationaal ministerie van buitenlandse zaken, … We begrijpen maar al te goed dat dit een ingewikkeld en tijdsintensief karwei is. Sirius Legal beschikt over een omvangrijk netwerk van buitenlandse advocaten gespecialiseerd in deze materies. Zo kunnen we voor bijna elk derde land onze eigen 'gepastheidsbeoordeling' maken.

- **Stap 5**: beoordeel of SCCs volstaan. Nu je op de hoogte bent van de juridische situatie in het derde land is het tijd om te beoordelen of de standaard contractuele clausules (SCCs) volstaan. Deze zijn in het leven geroepen door de Europese Commissie voor gegevensexport naar derde landen. Het zijn overeenkomsten die je kan sluiten met de verwerkingsverantwoordelijke of verwerker in dat derde land. Als er geen problemen werden gevonden in de bovenstaande stap, dan kan je deze SCCs zonder meer gebruiken. Hou wel in het achterhoofd dat de Europese Commissie deze SCCs aan het herzien zijn. Als de SCCs niet volstaan, ga dan naar de volgende stap.
- **Stap 6**: creëer aanvullende garanties en gebruik aangepaste SCC's. De gegevensbeschermingsautoriteit van Baden-Württemberg stelt een aantal aanvullende garanties voor. Ten eerste de encryptie (versleuteling) van de gegevens aan jouw kant. Zorg er in dat geval voor dat jij als exporteur de enige bent met de 'sleutel' om de gegevens te ontcijferen en dat de encryptie niet zomaar kan worden ontsleuteld. We nodigen je uit om het artikel "Is encryptie verplicht onder GDPR?" te lezen als je meer wil weten over encryptie. Ten tweede de anonimisering of pseudonimisering van de gegevens aan jouw kant. Zo zorg je ervoor dat de ontvanger van de gegevens niet zomaar kan weten over wie het nu werkelijk gaat. Denk eraan dat dit proces vaak al begint voor je de gegevens nog maar ingeeft of ergens uploadt. Vervolgens stelt de gegevensbeschermingsautoriteit van Baden-Württemberg een aantal concrete aanpassingen en aanvullingen voor op de SCCs:
    - » Een verplichting voor de gegevensexporteur om de betrokkene te informeren dat zijn of haar gegevens naar een derde land gaan dat geen passend beschermingsniveau biedt;
    - » Een verplichting voor de gegevensimporteur om zowel de exporteur als de betrokkene op de hoogte te brengen van elk verzoek tot inzage van de gegevens. Als dit niet mogelijk is, de verplichting om de nationale gegevensbeschermingsautoriteit van de exporteur hiervan op de hoogte te brengen;
    - » Een verplichting voor de gegevensimporteur om juridische stappen te nemen tegen elk verzoek om inzage en deze uit te putten;
    - » De toekenning van meer rechten aan de betrokkene in een geschil met de gegevensimporteur en de toevoeging van een compensatieclausule.
- **Stap 7**: en als dat allemaal niet helpt… Het is mogelijk dat alle bovenstaande maatregelen ofwel niet mogelijk zijn ofwel nog steeds onvoldoende waarborgen bieden. In dat geval vermeldt de gegevensbeschermingsautoriteit van Baden-Württemberg dat er nog een alternatieve optie bestaat, maar dat deze alternatieven heel strikt geïnterpreteerd worden en dus weinig aanvaard als reden om gegevens te exporteren naar een derde land. Hieronder valt bijvoorbeeld de mogelijkheid om de toestemming van de betrokkene te vragen voor de gegevensexport. Deze toestemming moet wel voldoen aan alle vereisten van de GDPR. Met andere woorden: de toestemming moet vrij zijn, specifiek, geïnformeerd en ondubbelzinnig. Als al het bovenstaande niet heeft mogen baten is het allicht veiliger om de samenwerking met de partner te stoppen.

Dataveiligheid en cyber security

Uit het Cyber Readiness Report 2021 van verzekeraar Hiscox Group, blijkt dat maar liefst 42% van de Belgische ondernemingen in 2020 het voorwerp was van een cyberaanval. België scoort daarmee vér beneden het gemiddelde in West-Europa. De 8 belangrijkste landen om ons heen doen het stuk voor stuk véél beter als het gaat om cyberveiligheid. Bovendien voorzien specialisten dat de dreiging die uitgaat van cyberrisico's zoals hackingaanvallen of ransomware attacks in de toekomst alleen maar exponentieel zal toenemen.

Cyber security is dus zonder de minste twijfel een acuut aandachtspunt voor alle ondernemers, maar in de eerste plaats nog véél meer voor digitale ondernemers en voor al wie investeert in AI en Machine Learning-oplossingen. Het ergste wat je als onderneming kan overkomen, is dat de zorgzaam opgebouwde AI-kennis en de grote investeringen die daarmee gepaard gaan, in één trek verloren zouden gaan door bijvoorbeeld een ransomware aanval.

Cyberveiligheid maakt geen onderscheid tussen AI-toepassingen en klassieke bedrijven, natuurlijk, maar toch zijn er enkele specifieke risico's waar je in het kader van AI-projecten maar beter oog voor kan hebben.

- Ransomware. Bedrijven die het slachtoffer worden van ransomware, komen helaas steeds vaker voor. Ransomware is schadelijke software, vaak geüpload naar computers via e-mailbijlagen, die vervolgens gevoelige gegevens kan stelen of deze kan gijzelen totdat je losgeld betaalt aan de dader. Heel wat bedrijven wereldwijd zijn al het slachtoffer van ransomeware geweest en vaak bleven hun deuren daardoor wekenlang, zelfs maandenlang gesloten of ging een schat aan waardevolle bedrijfsdata (ook uit AI-toepassingen) definitief verloren.
- Zwak wachtwoordgebruik. Eén van de meest voorkomende manieren waarop gegevens worden gestolen, geopend of gecompromitteerd, is een gebrek aan paswoordveiligheid of het gebruik van zwakke wachtwoorden. Bedrijven die nalaten sterke wachtwoorden te gebruiken, hetzelfde wachtwoord voor software en systemen gebruiken of hun wachtwoorden niet regelmatig bijwerken, brengen hun bedrijf nodeloos in gevaar.
- Ongelukjes. Vaak is het verlies of het onbedoeld delen van bestanden en gegevens binnen bedrijven gewoon het gevolg van menselijke fouten. Beveiligingsproblemen kunnen het gevolg zijn van slordigheid en onachtzaamheid, van zwakke wachtwoorden, onbeveiligde wifi, verlies van fysieke bestanden of klikken op geïnfecteerde bestanden en e-mailbijlagen. Permanente awareness en voorlichting van personeelsleden is dan ook de hoeksteen van een goed veiligheidsbeleid.
- Virussen. Virussen evolueren permanent. Antivirussoftware werkt ijverig om deze steeds veranderende cyberbeveiligingsdreiging bij te houden. Het is dan ook belangrijk om de meest up-to-date virussoftware gebruiken om het gevaar te minimaliseren. Computervirussen kunnen immers ernstige schade toebrengen aan bedrijfsgegevens en eigendommen door data te wissen, de prestaties te vertragen, programma's te beschadigen, je harde schijf opnieuw te formatteren, bestanden te verwijderen, ...
- Verouderde technologie. Technologie evolueert voortdurend en dus veranderen ook veiligheidsrisico's permanent. Verouderde software en technologie is dus een absoluut te mijden risico. Desondanks zien we in héél wat bedrijven nog steeds verouderde besturingsprogramma's, verouderde hardware, softwareupdates die niet afgedwongen worden bij medewerkers, ...
- Afstandswerk. Thuiswerk is een nieuwe realiteit in deze coronatijden, maar medewerkers op locatie of thuis laten werken kan wel aanzienlijke extra beveiligingsproblemen opleveren voor letterlijk élk bedrijf. Die risico's komen voort uit het gebruik van onbeveiligde wifiverbindingen, zwakke firewalls, privégebuik van professionele toestellen, ...

Dit alles geldt zo mogelijk nog meer voor AI-toepassingen, die per definitie digitaal zijn én in quasi alle gevallen ook omwille van hun aard in een connected omgeving functioneren, waardoor zij zich al evenzeer bijna per definitie blootstellen aan cyberrisico's.

Nochtans zijn er voor ondernemingen, ook voor kleinere met beperkte budgetten, oplossingen om je bedrijf, of meer specifiek je AI-toepassing, ook digitaal beter te beschermen.

Enkele standaardbeveiligingspraktijken die alle bedrijven, en zéker bedrijven die met AI aan de slag gaan, zouden moeten overwegen, zijn:

- Een overkoepelend informatieveiligheidsaudit en -plan voor het voorkomen van en omgaan met cyberbeveiliging binnen het bedrijf (veiligheid van mailservers, gebruikte software, paswoordbeleid, toegangscontrole tot documenten, wifi en bedrijfsnetwerk…);
- Duidelijke en strenge interne richtlijnen rond mailverkeer, thuis- en afstandswerk, privégebruik van professionele toestellen, gebruik van clouddiensten, ... ;
- Opleiding, voorlichting en bewustmaking van personeelsleden. Een software- en hardwareinventaris opstellen met gebruikerslijsten en idealerwijze tracking en logging van gebruik;
- Antivirussoftware onderhouden op alle apparaten;
- Encryptie waar mogelijk;
- Vermijden van data-export buiten de EU waar mogelijk;
- Veilige opslag van je data ("on premise" beveiligd of via een betrouwbare cloud service);
- Gegarandeerde, betrouwbare en snelle back-ups;
- Kies voor het doorlopen van een cybersecurity verbetertraject én van een GDPR compliance audit;
- Stel een veiligheidsverantwoordelijke (DPO eventueel ook) aan die kan plannen en interne controles kan uitvoeren op het naleven van policies.

Goede contracten

Onze huidige wetgeving kent geen specifieke regels voor de aansprakelijkheid voor schade die voortvloeit uit het gebruik van AI-systemen. Maar outsourcing van heel wat bedrijfsinformatie en -taken komt steeds meer voor en daarvoor wordt steeds vaker AI ingezet.

Door middel van verschillende AI-toepassingen zal je als bedrijf meer data, in vele gevallen ook vertrouwelijke data, delen met (AI-)softwaredienstverleners. In die context zijn goede contracten en goede afspraken essentieel.

We hadden het al over omgaan met persoonsgegevens en over cybersecurity. In dit domein kan je met een technische partner zeker het nodige voorzien. Meer nog, als jouw projectpartner niet spontaan zelf de nodige waarborgen biedt op vlak van dataveiligheid, vraag je dan tijdig af of dit wel de gepaste, professionele partner is voor jouw project. Maturiteit rond dataveiligheid is immers een goede graadmeter voor de professionaliteit van élke IT-dienstverlener.

Maar waarop kan je nog meer letten in projectafspraken en contracten met developers en technische partners? Wel, we geven als laatste hoofdstuk in deze bijdrage nog zeven nuttige tips voor contracten in AI-projecten mee:

- Ga voorbereid in onderhandeling. Zorg dat je zicht hebt op je eigen situatie: hoe gevoelig is je bedrijfsinformatie en welke impact heeft dit op je onderneming wanneer er zich een incident voordoet? Zijn de aangeboden beveiligingsmaatregelen daar toereikend genoeg voor? Wat is de bereidheid van de AI-dienstverlener om zich aan te passen aan jouw beveiligingseisen? Kijk na in hoeverre de dienstverlening conform je eigen veiligheidsbeleid en -procedures is. Zorg ook dat je tijdig een DPIA uitvoert als jouw project de verwerking van persoonsgegevens onder GDPR omvat. Zo'n DPIA is de ideale manier om de scope en risico's van je project in kaart te brengen.
- Zorg voor zeer duidelijke afspraken over timings, projectduur, vertragingen en de eventuele schadevergoedingen die daaruit voortkomen. Heel wat software developmenttrajecten lopen vertraging op en dat is voor AI- of ML-trajecten niet anders. En even vaak zien we dat er geen duidelijke afspraken gemaakt werden bij de start van het project, wat al snel tot hele grote frustraties en vaak ook het vastlopen van samenwerkingen zorgt. Maak vooraf afspraken: goede afspraken maken goede vrienden.
- Hou rekening met specifieke wetgeving voor jouw bedrijf of jouw data. We hadden het al over GDPR voor wat betreft persoonsgegevens, maar AI-trajecten komen ook steeds vaker in het vaarwater van consumentenbescherming, mededingingsrecht of andere wetgeving die beperkingen kan opleggen aan wat jij kan en mag in de context van AI-projecten. Denk maar aan de vele transparantie-, meldings-, notificatie- en medewerkingsverplichtingen die op je onderneming van toepassing kunnen zijn, afhankelijk van de soort data die je verwerkt, de sector waarin je werkzaam bent of de hoedanigheid van je onderneming.
- Zorg voor duidelijke afspraken over intellectuele eigendom. IP is cruciaal in AI-trajecten. De eerste vraag is wie eigenaar is of wordt van de ontwikkelde tool. Wordt jouw bedrijf eigenaar of krijgt het slechts een licentie of gebruiksrecht op hetgeen ontwikkeld wordt? Die laatste optie is vaak goedkoper, maar als jouw leverancier verdwijnt, failliet gaat of gewoon stopt met de verdere terbeschikkingstelling van de tool waar jouw bedrijf zwaar op steunt, heb je voor je het weet, grote problemen op vlak van continuïteit. Een andere, juridische gezien overigens erg boeiende vraag, is ook wie eigenaar is van de output die gecreëerd wordt door AI-systemen? De "uitkomst" van berekeningen door een algoritme kan immers in theorie bijvoorbeeld auteursrechtelijk beschermbare content zijn, maar wie er dan de auteur of eigenaar van is, is hoogst onduidelijk. Zelflerende algoritmes kunnen op zichzelf immers geen auteur zijn en de zoektocht naar de

eigenaar van de output dreigt zo voor problemen te zorgen. Tenzij je een en ander gewoon netjes contractueel regelt, natuurlijk. Zorg ook voor de nodige garanties van je partner voor elk gebruik van reeds bestaande softwarecode, algoritmes, ideeën of concepten. Voor je het weet komt er een ander bedrijf aankloppen dat beweert dat jij inbreuk maakt op hun rechten en ook hier geldt dat goede afspraken in dat geval veel discussies kunnen voorkomen.

- Zorg voor goede SLA's en voor goede onderhouds- en supportverplichtingen, zéker bij beveiligingsincidenten, waar je erg veel voordeel zal halen uit goed omschreven detectieplichten, waarschuwingsplichten en medewerkingsplichten, in combinatie met goede schadebedingen voor het geval de gemaakte afspraken toch niet gevolgd worden. Stel bijvoorbeeld ook in het kader van de opstelling van een incident response team vast welke coördinerende rol de AI-dienstverlener kan opnemen. Voeg daaraan toe welke communicatie de AI-dienstverlener wel, maar vooral niet kan voeren en zorg ervoor dat je deze crisiscommunicatie zelf in handen houdt.
- Maak goede afspraken over verplichtingen rond updates en upgrades en de daaraan verbonden timings en kosten, de aansprakelijkheid van de AI-dienstverlener en zijn verplichtingen tot vrijwaring in geval van schadeclaims, boetes en overige vervolgingen waar je je aan zou kunnen blootstellen.
- Confidentialiteit is vanzelfsprekend érg belangrijk als je bedrijfskritische data toevertrouwt aan een externe partner. Zorg dus voor goede confidentialiteitsverplichtingen én voor goede niet-concurrentiebedingen. Je wil wellicht liever niet dat je huidige supplier morgen de bij jou opgedane kennis gaat rentabiliseren bij één van je directe concurrenten.

Besluit

In deze snel evoluerende wereld van zelfrijdende auto's, medische robots en slimme marketing algoritmes, staan we aan de vooravond van een echte revolutie. Als slimme ondernemer bereid je je best tijdig voor op een nieuwe economie die nog meer dan ooit op kennis en inzicht gebaseerd zal zijn. Start dus zeker tijdig en laat jouw bedrijf meesurfen op de AI-golf. Maar wees ook voorzichtig. Aan de slag gaan met AI brengt een héle hoop juridische vragen en uitdagingen met zich mee. Laat je tijdig bijstaan door een specialist, zodat je geen onnodige juridische risico's neemt die van jouw grote AI-project potentieel een mislukking kunnen maken.

COLOFON

Artificiële intelligentie in Marketing: ook voor de KMO
Met welke legale aspecten moet je rekening houden?

www.siriuslegal.be
Veemarkt 70, 2800 Mechelen

In opdracht van Odisee vzw
Warmoesberg 26, 1000 Brussel

In het kader van het tetra-onderzoeksproject Start2AIM, met steun van VLAIO.

Odisee
DE CO-HOGESCHOOL