

# 7 NUTTIGE TIPS VOOR GOEDE CONTRACTEN IN AI-PROJECTEN

## Tip 1: 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.

## Tip 2: 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.

## Tip 3: 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.

## Tip 4: 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.

 **Tip 5: Zorg voor goede SLA's en voor goede onderhouds- en supportverplichtingen.**

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, waarschuwingplichten 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.

 **Tip 6: Maak goede afspraken over verplichtingen rond updates en upgrades.**

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.

 **Tip 7: Zorg dus voor goede confidentialiteitsverplichtingen.**

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 leverancier morgen de bij jou opgedane kennis gaat rentabiliseren bij één van je directe concurrenten.