



Maak kennis met

Dirkzwager

legal & tax

Dirkzwager
legal & tax



Juridische aspecten bij inkoop E-Health

NEVI Zorg Congres 8-2-2019

Inleiding

- Inkopen van eHealth: verschillende onderwerpen
 - Samenwerking
 - Laten ontwikkelen van software
 - big data toepassingen: eigendom van data?
- Hoe pak je de inkoop van eHealth oplossingen aan
 - Formule voor een goed contract
 - Risico/impactanalyse
 - SaaS

Centrale casus

- Een specialist heeft een idee om een app te ontwikkelen.
- Met big data analyses bepaalt het algoritme in de software welke patiënten direct een vervolgspraak moeten plannen en welke niet.
- De specialist zoekt een IT-leverancier die de app kan ontwikkelen.
- Het ziekenhuis betaalt de IT-leverancier.

- Welke juridische aspecten spelen hier?

Samenwerking?



- Er wordt veel “samengewerkt”
- Samenwerking vergt geven en nemen en win/win
 - Ziekenhuis / specialist verstrekt data
 - Leverancier bouwt app
- En als het klaar is?
 - Samen exploiteren?
 - Of alleen het ziekenhuis/specialist?
 - Gezamenlijk eigendom? Waarop dan?

Samenwerkingsovereenkomsten

Inbreng van partijen loopt uiteen, bijv.:

- Materieel: geld (sponsoring) of “in kind” (faciliteiten, personeel)
- Immaterieel: IE-rechten, kennis en ervaring (“know how”) en datasets

Immaterieel:

- ‘**Background**’: bestaande data, kennis en IE ingebracht in de samenwerking
- ‘**Foreground**’: nieuwe data, kennis en IE gedurende samenwerking ontstaat

Duidelijke afspraken noodzakelijk wie wat met wat mag doen:

- Maar eerst inventariseren:
- Wélke kennis en IE bestaat al?
- Welke data worden beschikbaar gesteld? Mag dat wel?

Softwareontwikkeling



Aan wie komen de rechten op de software toe?

- **Specialist** want die had het idee, de rest voert alleen maar uit of betaalt alleen maar.
- **IT-leverancier** want die bouwt immers
- **Ziekenhuis** wat dat betaalt alles

Antwoord:

- **IT-leverancier**
- De auteursrechten op de software komen toe aan de maker (2 Aw). Dus de programmeur, althans zijn werkgever (7 Aw).
- Tenzij: vooraf schriftelijk overgedragen aan opdrachtgever

Aandachtspunten Big Data in zorg

Veel aandacht voor privacy maar er is meer

- Gegevens zeer (privacy)gevoelig
- Wetenschappelijk vs commercieel onderzoek?
- Betrouwbaarheid en veiligheid bronnen/data?
- Conclusies enkel op basis van relaties?
- Dominantie van grote marktpartijen (Google, Apple, Facebook, Philips, Siemens, etc)?
- Kun je toegang tot data afdwingen?
- Eigendom van data?



Eigendom van data?

Terug naar de casus: Van wie zijn de data?

- Van de **specialist**? (Want hij heeft ze samengesteld/geselecteerd?)
- Van het **ziekenhuis**? (Want data zijn toch opgeslagen op haar servers?)
- Van de **IT-leverancier**? (Want software gemaakt om van data informatie te maken?)
- Van de **patiënt**? (Gaaf toch immers om gegevens over hem/haar?)

Antwoord: hangt er van af.....

- Eigendom op data *sec* bestaat niet.
- ‘Eigendom’ = meest omvattende recht van persoon op een zaak (5:1 BW).
- Een ‘zaak’ = voor menselijke beheersing vatbaar stoffelijk object (3:2 BW)
- Data als zodanig is niet stoffelijk (de drager waarop data staan wel).
- Voordeel van eigendom: werkt tegenover iedereen (‘absolute werking’).

Dus data zijn van niemand / vogelvrij?

Nee! Kijken naar de concrete verschijningsvorm van de data:

- Bescherming data als **persoonsgegevens**: geen eigendomsrecht meer wel vergaande rechten van betrokkenen (inzage, correctie, verwijdering, portering, etc).
- Bescherming dataset door **atabankenrecht**: intellectueel eigendomsrecht dat (substantiële) investering beschermt van verzameling van gegevens.
- Bescherming data door **auteursrecht**: (onderzoeks)rapporten, tekeningen, uitgeschreven analyses en software. Komen toe aan maker (of zijn werkgever).
- Bescherming data door **octrooirecht**: IE-recht dat data als onderdeel van werkwijze of uitvinding kan beschermen.
- Bescherming data als **bedrijfsgeheim** (nieuw 2018): geen eigendomsrecht, maar wel handhavingsrechten op geheime kennis of knowhow (recepturen, algoritmen).
- Bescherming data via **contract**: kan, maar werkt alleen tussen contractanten

Tip: inventariseer wat de data zijn en hoe die beschermd kunnen zijn

Risico's bij samenwerking?

Ruzie krijgen:

Nietes, mijn bijdrage was belangrijker / groter / meer, dus alles is van mij

Het was mijn idee dus alles wat volgde is dus van mij.

ECHT NIET! Jij deed niets, ik moest alles doen, dus alles is van mij!!

Geheimen verspreiding zich makkelijk, bijv.:

- in exemplaren, prototypes, beschrijvingen, foto's e.d. (fysiek of digitaal);
- “wandelende kennis” via kennisoverdracht en ervaring projectmedewerkers;
- Partijen vaak onbekendheid met eigen bedrijfsgeheim daardoor geen zicht op weglekken (technisch procedé, werkmethode, functionaliteit software, klanten gegevens, verzameling data uit onderzoek, of gewoon ervaring hoe je iets doet)

Tegenmaatregelen

Afspraken over wie, wat doet en inbrengt en aan wie de resultaten toekomen:

- Goede afspraken over rol van deelnemers (wie, wat, wanneer, hoe)
- Aansturing en regie vastleggen (via stuurgroep, projectgroep)

Feitelijke beschermingsmaatregelen bij geheimhouding:

- Achter slot en grendel, fysiek en digitaal (encryptie).
- Toegang op '*need to know*' basis (autorisaties, login codes).
- Beveiligingsinstructies personeel (beleid, *mindset*, training, interviews).
- Betrokkenheid HR- en IT-afdelingen bij realisatie bescherming.

Maar wat als de kennis 'vloeibaar' is?

- Schriftelijke afspraken maken met betrokken partijen en werknemers (NDA);
- HR en projectmanager belangrijke rol bij *onboarding* en *exit* medewerkers!
- Sluit een schriftelijke NDA met alle betrokken (rechts)personen!

Dwarsdoorsnede van een Non Disclosure Agreement

Considerans	Uitleg context en doel waarom geheime kennis wordt verstrekt; belang van geheimhouding aangeven; aangeven wat follow up is als doel is gerealiseerd.
Definitie	Wat is “Vertrouwelijke Informatie”: alles, niet alles?
Geheimhouding	Vertrouwelijke Informatie niet aan ongeautoriseerde derden verstrekken; doorleggen aan derden (+ werknemers)
Onthouding	“Restricted Use”: Verbod ander gebruik dan beoogde doel (in verband met de samenwerking, of alleen voor onderzoek product of ook voor exploitatie); doorleggen aan derden (+ werknemers)
Retournering/ Vernietiging	Bij einde samenwerking alles teruggeven of vernietigen.
Looptijd	Geheimhouding en onthouding na einde looptijd?
Boete	Prikkel tot afschrikking of gefixeerde schadevergoeding?
Overig	Toepasselijke recht, bevoegde rechter

Afspraken maken dus belangrijk

Hoe doe je dat? Formule = (W+W+W+H+K) + (R*I)/tegenmaatregel

Vastleggen van **toetsbare** afspraken

- **Wat** moet worden gedaan?
- Door **Wie** moet Wat worden gedaan?
- **Wanneer** moet Wie Wat doen?
- **Hoe** moet Wie Wat Wanneer doen?
- Wat **Kost** het Wat door Wie, Wanneer en Hoe?

Daarnaast concrete risico's adresseren door procedurele, praktische of juridische afspraken.

- **Risico * Impact** / tegenmaatregel

Onderwerp	Vertaling naar contract
Wat?	Leveringsomvang: Specificaties / Programma van Eisen / Resultaten (BVP) / SLA (bij onderhoud en beheer)
Wie?	Wat doet leverancier, wat doet afnemer? Vastleggen onderlinge verantwoordelijkheden in contract of bijlage (Plan van Aanpak)
Wanneer?	Hoe belangrijk zijn termijnen: fatale termijnen? Versterken met boete? Bij samenwerking: goede planning en afstemming noodzakelijk. Tussentijdse milestones? (Planning)
Hoe?	Hoe kom je van A naar B? Vastleggen in Plan van Aanpak of Installatie/Implementatieplan, inplannen resources.
Wat kost het?	Ga je uit van offerte van leverancier (let op kleine lettertjes) of maak je na onderhandeling prijsblad met actuele prijzen?
Risico 1	Wat is het risico, wat kun je doen om intreden risico te voorkomen? Welke afspraak maak je en waar leg je dit vast?
Risico 2	Etcetera

Risico-inventarisatie

Wat ga je doen? ICT-contracten soms lastig te typeren:

- Hardware (koop/huur/lease?)
- Software (klassieke licentie of SaaS/PaaS/laaS?)
- Diensten (installatie “on premise” of “in the cloud”; beheer en onderhoud, trainingen, implementatie; tijdelijk inhuur mensen; outsourcing?)
- Ontwikkeling maatwerk of implementatie standaard?
- Samenwerking of levering? Open source?

Welke concrete risico's vloeien hieruit voort?

- Levering en omvang, project, doorlooptijd, continuïteit, etc
- Impactanalyse (kans * impact = meer/minder actie)

Business Case SaaS ter illustratie

‘Software as a Service’ (wikipedia):

- *is **software die als een online dienst** wordt aangeboden. [...] De **SaaS-aanbieder zorgt voor installatie, onderhoud en beheer**, de gebruiker **benadert de software over het internet** bij de SaaS-aanbieder. [...] SaaS wordt gezien als de applicatielaag van [cloud computing](#), waarbij het platform (PaaS) en de infrastructuur (IaaS) als onderliggende lagen worden toegepast. Zonder deze onderliggende lagen is er geen sprake van **flexibel verhogen of verlagen van het verbruik / de gebruikers**.*

Kenmerken SaaS

Belangrijkste kenmerken SaaS (Software as a Service)

- Standaardsoftware (Geen/nauwelijks maatwerk, wel inrichten)
- Installatie niet 'on premise' maar bij derde (datacenter)
- Abonnement (pay per use(r))? Flexibiliteit (op-/afschalen gebruikers)? Wordt zeker niet altijd toegepast (en is zeker ook niet altijd nodig!)

Aandachtspunten:

- Afhankelijkheid keten: Leverancier maakt gebruik van derden, zoals datacenter en hostingleverancier, daarnaast nog telco's, datatransport etc.
- Continuïteit van dienstverlening

Risico-/impactanalyse

Stappenplan:

- Stap 1: eerst gehele project in kaart brengen
 - Fase 1: voorbereiding / ontwikkeling
 - Fase 2: installatie en inrichting
 - Fase 3: gebruik + onderhoud + beheer
 - Fase 4: einde overeenkomst
- Stap 2: per fase inzoomen op concrete risico's
- Stap 3: impactanalyse (kans * impact = prioriteit)
- Stap 4: prioriteiten sorteren (hoog-laag)
- Stap 5: praktische oplossingen voor risico's

Risico per fase (voorbeeld)	Kans (1-5)	Impact (1-5)	Prio	Tegenmaatregel (zo praktisch mogelijk maken)
Fase 1: voorbereiding				
Software sluit niet aan op eisen en wensen	3	5	15	<ul style="list-style-type: none"> - Verschillenanalyse verrichten tussen mogelijkheden software en eisen en wensen - <i>Proof of concept</i> uitvoeren - Daarna programma van eisen en wensen fixeren
Fase 2: implementatie				
Project loopt uit	3	3	9	<ul style="list-style-type: none"> - Onaantrekkelijk maken van uitloop door fatale termijnen (kunt sneller ontbinden of schadevergoeding vorderen) - Heldere planning opstellen met duidelijke verdeling van verantwoordelijkheden - Actief bewaken van de planning. Leverancier hoofdverantwoordelijk maken hiervoor.
Fase 3: gebruik, beheer en onderhoud				
Externe server valt uit/storing datacentrum	3	5	15	<ul style="list-style-type: none"> - Uitwijk naar tweede server of tweede datacentrum (moet dus wel geconfigureerd zijn en klaar staan) - Backup data beschikbaar houden

Risico per fase (voorbeeld)	Kans (1-5)	Impact (1-5)	Prio	Tegenmaatregel (zo praktisch mogelijk maken)
Fase 4: einde overeenkomst				
Discontinuïteit dienstverlening door niet tijdige overstap op nieuwe leverancier	2	5	10	<ul style="list-style-type: none"> - Goede exitregeling afspreken (post-contractuele afspraak): medewerking tegen redelijke kosten - Verlenging licentie opnemen voor beperkte duur na beoogd einde van de overeenkomst
Overig				
Datalek	2	3	6	<ul style="list-style-type: none"> - Beveiligingsmaatregelen specificeren (wat is passend?) - Vooraf afspraken maken over meldingsprocedure in verwerkersovereenkomst
Leverancier failliet en curator wil niet meewerken	3	4	12	<ul style="list-style-type: none"> - Externe of lokale back-up (niet bij failliet) - Eigen hardware inzetten (niet van failliet) - Instappen derde (driepartijenovereenkomst) - Verzekeren (SaaS escrow)
Vendor lock-in	3	4	12	<ul style="list-style-type: none"> - Service Levels in SLA? - Inperken opschortingsrecht leverancier - Opzegmogelijkheid hebben - Exit-regeling (medewerking, afgifte data, verlenging licentie)

Dwarsdoorsnede van IT-contract	Wat regel je?
Overwegingen	Doel van de overeenkomst
Definities	Gelijke terminologie gebruiken
Onderwerp	Wat -vraag, eventueel koppeling met AV, rangorde
Levering, implementatie, opleiding	Wanneer , door Wie en Hoe
Acceptatieprocedure	Controle of (deel)levering voldoet aan wat-vraag
Onderhoud en beheer (volgens SLA)	Dicteert Wat, Hoe, Wanneer-vraag na Acceptatie
Governance en evaluatie	Aansturing project + contractmanagement
Prijs en betaling	Gefaseerde betaling belangrijk drukmiddel!
Garantie en aansprakelijkheid	Garantie en beperking aansprakelijkheid
Verwerking van persoonsgegevens	Extra nadruk bij SaaS, Cloud (bewerkschap)
Intellectuele eigendom	Licentie, vrijwaring tegen claims derden
Duur, beëindiging en gevolgen	Looptijd, opzegging, ontbinding, exit-regeling
Toepasselijk recht en geschillen	Nederlands recht, rechter/arbiter/mediation

Lessen om mee te nemen

- Samenwerken of levering?
- Inventariseer aan wie wat toekomt. Maak afspraken over data!
- Zijn kernvragen (wat, wie, wanneer, hoe, kosten) beantwoord?
- Maak een risico-/impact-analyse!
- SaaS: niet anders aanpakken dan andersoortige projecten. Accentverschil:
 - nadruk op manieren om continuïteit dienstverlening te borgen
 - Nadruk op inperken afhankelijkheid (inperken opschorting, opzegmogelijkheid exitregeling)
- Actief contractmanagement: leg contract niet in de la, maar houdt deze “stand-by”.

Contactpersoon : Ernst-Jan van de Pas
E-mail : vandePas@dirkzwager.nl

Dirkzwager

legal & tax

Kantoor Arnhem
Postbus 111
6800 AC Arnhem
Velperweg 1
6824 BZ Arnhem

Kantoor Nijmegen
Postbus 55
6500 AB Nijmegen
Van Schaeck Mathonsingel 4
6512 AN Nijmegen

T +31 (0)88 24 24 100

F +31 (0)88 24 24 111

E info@dirkzwager.nl

I www.dirkzwager.nl